

# **AT-AR256E v3**

4 Ports ADSL2/2+ Router

User Manual

**Copyright © 2008 Allied Telesis, Inc.**

All rights reserved. No part of this publication may be reproduced without prior written permission from Allied Telesis, Inc.

Microsoft and Internet Explorer are registered trademarks of Microsoft Corporation. Netscape Navigator is a registered trademark of Netscape Communications Corporation. All other product names, company names, logos or other designations mentioned herein are trademarks or registered trademarks of their respective owners.

Allied Telesis, Inc. reserves the right to make changes in specifications and other information contained in this document without prior written notice. The information provided herein is subject to change without notice. In no event shall Allied Telesis, Inc. be liable for any incidental, special, indirect, or consequential damages whatsoever, including but not limited to lost profits, arising out of or related to this manual or the information contained herein,



## SAFETY NOTICE

- ✓ Do not open service or change any component.
- ✓ Only qualified technicians are allowed to service the equipment.
- ✓ Observe safety precautions to avoid electric shock
- ✓ Check voltage before connecting to the power supply.  
Connecting to the wrong voltage will damage the equipment.

## LIMITATION OF LIABILITY AND DAMAGES












THE PRODUCT AND THE SOFTWARES WITHIN ARE PROVIDED "AS IS," BASIS. THE MANUFACTURER AND MANUFACTURER'S RESELLERS (COLLECTIVELY REFERRED TO AS "THE SELLERS") DISCLAIM ALL WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, INCLUDING WITHOUT LIMITATION THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, OR ANY WARRANTIES ARISING FROM COURSE OF DEALING, COURSE OF PERFORMANCE, OR USAGE OF TRADE. IN NO EVENT WILL THE SELLERS BE LIABLE FOR DAMAGES OR LOSS, INCLUDING BUT NOT LIMITED TO DIRECT, INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL, EXEMPLARY, OR CONSEQUENTIAL, DAMAGES, DAMAGES FOR LOSS OF BUSINESS PROFITS, OR DAMAGES FOR LOSS OF BUSINESS OF ANY CUSTOMER OR ANY THIRD PARTY ARISING OUT OF THE USE OR THE INABILITY TO USE THE PRODUCT OR THE SOFTWARES, INCLUDING BUT NOT LIMITED TO THOSE RESULTING FROM DEFECTS IN THE PRODUCT OR SOFTWARE OR DOCUMENTATION, OR LOSS OR INACCURACY OF DATA OF ANY KIND, WHETHER BASED ON CONTRACT, TORT OR ANY OTHER LEGAL THEORY, EVEN IF THE PARTIES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE ENTIRE RISK AS TO THE RESULTS AND PERFORMANCE OF THE PRODUCT OR ITS SOFTWARE IS ASSUMED BY CUSTOMER. BECAUSE SOME STATES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO THE PARTIES. IN NO EVENT WILL THE SELLERS' TOTAL CUMULATIVE LIABILITY OF EACH AND EVERY KIND IN RELATION TO THE PRODUCT OR ITS SOFTWARE EXCEED THE AMOUNT PAID BY CUSTOMER FOR THE PRODUCT.

# ELECTRICAL SAFETY AND EMISSIONS STANDARDS

This product meets the following standards.

U.S. Federal Communications Commission
<p>This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:</p> <p>This device may not cause harmful interference.</p> <p>This device must accept any interference received, including interference that may cause undesired operation.</p> <p>Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:</p> <ul style="list-style-type: none"> <li>- Reorient or relocate the receiving antenna.</li> <li>- Increase the separation between the equipment and receiver.</li> <li>- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.</li> <li>- Consult the dealer or an experienced radio/TV technician for help.</li> </ul>

Canadian Department of Communications
<p>This Class B digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.</p> <p>Cet appareil numérique de la classe B respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.</p>

CE Marking Warning
<p>This is a Class B product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.</p> <p><b>Important:</b> Appendix A contains translated safety statements for installing this equipment. When you see the  go to Appendix A for the translated safety statement in your language.</p> <p><b>Wichtig:</b> Anhang A enthält übersetzte Sicherheitshinweise für die Installation dieses Geräts. Wenn Sie  sehen, schlagen Sie in Anhang A den übersetzten Sicherheitshinweis in Ihrer Sprache nach.</p> <p><b>Vigtigt:</b> Tillæg A indeholder oversatte sikkerhedsadvarsler, der vedrører installation af dette udstyr. Når De ser symbolet , skal De slå op i tillæg A og finde de oversatte sikkerhedsadvarsler i Deres eget sprog.</p> <p><b>Belangrijk:</b> Appendix A bevat vertaalde veiligheidsopmerkingen voor het installeren van deze apparatuur. Wanneer u de  ziet, raadpleeg Appendix A voor vertaalde veiligheidsinstructies in uw taal.</p> <p><b>Important :</b> L'annexe A contient les instructions de sécurité relatives à l'installation de cet équipement. Lorsque vous voyez le symbole , reportez-vous à l'annexe A pour consulter la traduction de ces instructions dans votre langue.</p> <p><b>Tärkeää:</b> Liite A sisältää tämän laitteen asentamiseen liittyvät käännetty turvaohjeet. Kun näet -symbolin, katso käännettyä turvaohjetta liitteestä A.</p> <p><b>Importante:</b> l'Appendice A contiene avvisi di sicurezza tradotti per l'installazione di questa apparecchiatura. Il simbolo , indica di consultare l'Appendice A per l'avviso di sicurezza nella propria lingua.</p> <p><b>Viktig:</b> Tillegg A inneholder oversatt sikkerhetsinformasjon for installering av dette utstyret. Når du ser , åpner du til Tillegg A for å finne den oversatte sikkerhetsinformasjonen på ønsket språk.</p> <p><b>Importante:</b> O Anexo A contém advertências de segurança traduzidas para instalar este equipamento. Quando vir o símbolo , leia a advertência de segurança traduzida no seu idioma no Anexo A.</p> <p><b>Importante:</b> El Apéndice A contiene mensajes de seguridad traducidos para la instalación de este equipo. Cuando vea el símbolo , vaya al Apéndice A para ver el mensaje de seguridad traducido a su idioma.</p> <p><b>Obs!</b> Bilaga A innehåller översatta säkerhetsmeddelanden avseende installationen av denna utrustning. När du ser , skall du gå till Bilaga A för att läsa det översatta säkerhetsmeddelandet på ditt språk.</p>

# CONTENTS

Preface .....	9
Purpose of This Guide .....	9
How This Guide is Organized .....	9
Document Conventions .....	9
Contacting Allied Telesis .....	10
Online Support .....	10
Email and Telephone Support .....	10
Warranty .....	10
Where to Find Web-based Guides .....	10
Returning Products .....	10
Sales or Corporate Information .....	10
Management Software Updates .....	10
Tell Us What You Think .....	10
Chapter 1: Introduction .....	11
Requirements .....	11
Software .....	11
Hardware .....	11
Package Contents .....	11
Device Design .....	11
Back Panel .....	11
Front Panel .....	12
Chapter 2: About the Web User Interface .....	13
Accessing the Web User Interface .....	13
Web User Interface Components .....	13
Buttons .....	13
Menus .....	14
Chapter 3: Basic Menu .....	15
Home .....	15
Quick Start .....	15
LAN Configuration .....	16
Diagnostics .....	17
Chapter 4: Advanced Menu .....	18
WAN .....	18
New Connection .....	18
ADSL Modulation .....	22
Connection Scan .....	23
LAN .....	24
LAN Configuration .....	24
LAN Group Configuration .....	25
Assign ISP DNS, SNTP .....	26
LAN Clients .....	27
Applications .....	27
Universal Plug and Play (UPnP) .....	28
Simple Network Time Protocol .....	28
IGMP Proxy .....	29
TR-068 WAN Access .....	30
DNS Proxy .....	31
Dynamic DNS Client .....	31
Port Forwarding .....	32
Bridge Filters .....	34

Web Access Control .....	35
Quality of Service .....	36
Egress .....	36
Ingress .....	38
QoS Shaper Configuration .....	42
Policy Routing Configuration .....	45
Routing .....	47
Static Routing .....	47
Routing Table .....	48
System Password .....	48
Changing the System Password .....	48
Changing the Timeout Settings .....	49
Firmware Upgrade .....	49
Restoring the Default Settings .....	49
Chapter 5: Security Menu .....	50
IP Filters .....	50
LAN Isolation .....	51
Chapter 6: Status Menu .....	52
Connection Status .....	53
System Log .....	53
Remote Log .....	54
Network Statistics .....	55
DHCP Clients .....	56
QoS Status .....	56
Modem Status .....	57
Product Information .....	57
Chapter 7: Help Menu .....	58

## FIGURES

Figure 1: Back Panel.....	11
Figure 2: LEDs on front panel.....	12
Figure 3: Menu Bar.....	14
Figure 4: Basic Home menu.....	15
Figure 5: LAN Configuration.....	16
Figure 6: DSL Modem Test.....	17
Figure 7: Advanced menu.....	18
Figure 8: New PPPoE Connection Setup.....	19
Figure 9: New PPPoA Connection Setup.....	19
Figure 10: New Static Connection Setup.....	20
Figure 11: New DHCP Connection Setup.....	20
Figure 12: New Bridge Connection Setup.....	21
Figure 13: ADSL Modulation.....	22
Figure 14: Connection Scan.....	23
Figure 15: LAN Configuration.....	24
Figure 16: LAN Group Configuration.....	25
Figure 17: LAN Clients.....	27
Figure 18: UPnP.....	28
Figure 19: SNTP.....	28
Figure 20: IGMP Proxy.....	29
Figure 21: Enable WAN Access Update.....	30
Figure 22: DNS Proxy.....	31
Figure 23: Dynamic DNS Client.....	32
Figure 24: Port Forwarding.....	32
Figure 25: Bridge Filters.....	34
Figure 26: Web Access Control.....	35
Figure 27: Egress.....	37
Figure 28: Layer 2 Egress.....	37
Figure 29: Layer 3 Egress.....	38
Figure 30: Untrusted mode Ingress.....	39
Figure 31: Layer 2 Ingress.....	40
Figure 32: Layer 3 Ingress.....	41
Figure 33: Static.....	42
Figure 34: QoS Shaper Configuration.....	43
Figure 35: HTB Queue Discipline enabled.....	44
Figure 36: Low Latency Queue Discipline enabled.....	44
Figure 37: PRIOWRR enabled.....	45

Figure 38: Policy Routing Configuration .....	45
Figure 39: Static Routing .....	47
Figure 40: Routing Table .....	48
Figure 41: Security menu.....	50
Figure 42: IP Filters .....	50
Figure 43: LAN Isolation .....	51
Figure 44: Status menu .....	52
Figure 45: Connection Status.....	53
Figure 46: System Log .....	53
Figure 47: Remote Log Settings.....	54
Figure 48: Network Statistics – Ethernet.....	55
Figure 49: Network Statistics – DSL.....	55
Figure 50: DHCP Clients .....	56
Figure 51: QoS Status .....	56
Figure 52: Modem Status .....	57
Figure 53: Product Information .....	57
Figure 54: Help menu.....	58



# Preface

## Purpose of This Guide

This guide describes the AT-AR256E v3 4 Ports ADSL2/2+ Router Management interface for allowing users or network managers to correctly configure the router getting the most of it.

## How This Guide is Organized

This guide contains the following chapters and appendices:

- Chapter 1**      **Introduction**, describes the features, functions, LEDs, and ports on the equipment. Please refer to AT-AR256E Quick Setup Guide for information on how to install and setup the router.
- Chapter 2**      **About the Web User Interface**, introduces the web user interface general settings, how to select options and how to move among menus.
- Chapters 3-7**   Explain the usage of the various menus.

## Document Conventions

This guide uses several conventions that you should become familiar with before you begin to install the product:



### Note

A note provides additional information. Please go to the Allied Telesis website <http://www.alliedtelesis.com> for the translated safety statement in your language.



### Warning

A warning indicates that performing or omitting a specific action may result in bodily injury.



### Caution

A caution indicates that performing or omitting a specific action may result in equipment damage or loss of data.

# Contacting Allied Telesis

This section provides Allied Telesis contact information for technical support as well as sales and corporate information.

## Online Support

You can request technical support online by accessing the Allied Telesis Knowledge Base: <http://www.alliedtelesis.com/kb/>. You can use the Knowledge Base to submit questions to our technical support staff and review answers to previously asked questions.

## Email and Telephone Support

For Technical Support via email or telephone, refer to the Support & Services section of the Allied Telesis web site: <http://www.alliedtelesis.com/support/>.

## Warranty

For product registration and warranty conditions please visit Allied Telesis website: <http://www.alliedtelesis.com/support/warranty/>

## Where to Find Web-based Guides

The installation and user guides for all Allied Telesis products are available in portable document format (PDF) on our web site at [www.alliedtelesis.com](http://www.alliedtelesis.com). You can view the documents online or download them onto a local workstation or server.

## Returning Products

Products for return or repair must first be assigned a return materials authorization (RMA) number. A product sent to Allied Telesis without an RMA number will be returned to the sender at the sender's expense.

To obtain an RMA number, contact Allied Telesis Technical Support through our web site: <http://www.alliedtelesis.com/support/>.

## Sales or Corporate Information

You can contact Allied Telesis for sales or corporate information through our web site: <http://www.alliedtelesis.com/>. To find the contact information for your country, select Contact Us -> Worldwide Contacts.

## Management Software Updates

New releases of management software for our managed products are available from either of the following Internet sites:

- Allied Telesis web site: <http://www.alliedtelesis.com/support/software/>
- Allied Telesis FTP server: <ftp://ftp.alliedtelesis.com/>

If you prefer to download new software from the Allied Telesis FTP server from your workstation's command prompt, you will need FTP client software and you must log in to the server. Enter "anonymous" for the user name and your email address for the password.

## Tell Us What You Think

If you have any comments or suggestions on how we might improve this or other Allied Telesis documents, please contact us at <http://www.alliedtelesis.com>.

# Chapter I: Introduction

Congratulations for the purchase of your router. This router provides advanced features that allow you to access the phone service and the Internet through a single wired connection.



Please refer to the AT-AR256E Quick Setup Guide for information on how to install connect and initially setup the router.

## Requirements

Your computer must meet the following minimum requirements.

### Software

#### Operating System:

Any operating system can be used

#### Browser:

Internet Explorer 6.0/7.0

Netscape Navigator 3.02

### Hardware

233MHz processor

CD-ROM Drive

Ethernet network adapter

## Package Contents

Package contents include:

- Router
- Telephone cable
- Ethernet cable
- Power adaptor
- Documentation CD
- Quick Setup Guide

## Device Design

### Back Panel

The back panel provides ports to power up and connects the router to your network.

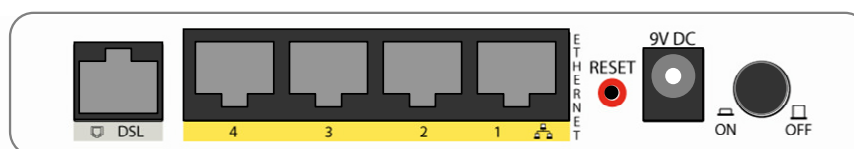


Figure I: Back Panel

Label	Used for...
DSL	Connecting the telephone cable
ETHERNET 1-4	Connecting the Ethernet cables
RESET	Resetting the router. Press and hold for 10 seconds to reset.

<b>9V DC</b>	Connecting the power adaptor
<b>ON/OFF</b>	Switching the router on/off

## Front Panel

The LEDs on the front panel give you an idea about the power and connection status.



**Figure 2: LEDs on front panel**

Label	Action	Description
<b>POWER</b>	Off	No power is supplied to the device
	Steady light	Connected to a AC power supply
<b>ETHERNET</b>	Off	No Ethernet connection
	Steady light	Connected to an Ethernet port
	Blinking light	Transmitting/Receiving data
<b>DSL</b>	Blinking light	Establishing DSL signal
	Steady light	DSL signal is established
<b>INTERNET</b>	Off	No Internet connection
	Steady light	Connected to the Internet
	Blinking light	Transmitting/Receiving data

## Chapter 2: About the Web User Interface

The Web User Interface is used to configure the router settings.

### Accessing the Web User Interface

To access the Web User Interface:

1. Open a browser.
2. Enter the router's IP address. The default IP address is **192.168.1.1**.
3. When authentication is enabled (default), the Log In page will appear. On the Log In page, enter the **Username** and **Password**. The default Username is **manager** and Password is **friend**.
4. Click **Log In**.

### Web User Interface Components

Buttons, commands and menus make up the browser-based user interface.

#### **Buttons**

##### Apply

Click to implement the configuration changes. Clicking Apply will not implement the changes when the router is restarted.

##### Cancel

Click to revert to the last saved configuration.

## Menus

The Web User Interface includes the following menus:

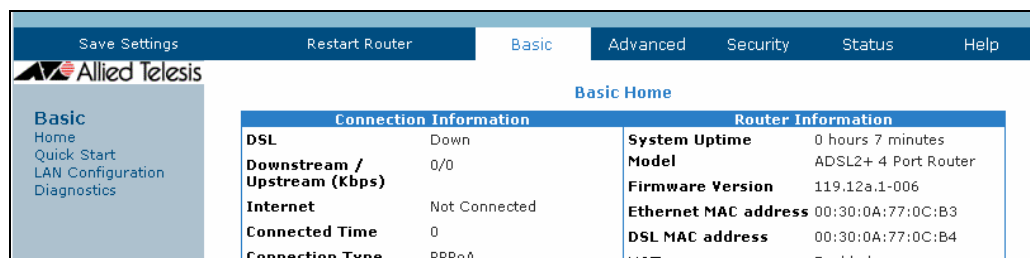


Figure 3: Menu Bar

### Save Settings

It isn't actually a menu but a command. Selecting it will make the router save the current settings, such that the router will be retained same configuration next time it is started.

### Restart Router

This menu item is a command too. Selecting it will make the router restart.

### Basic Menu

The Basic menu provides the Home, Quick Start, LAN Configuration and Diagnostics links.

### Advanced Menu

The Advanced menu provides advanced configuration settings for existing connections. At least one WAN connection must be configured before implementing advanced WAN configuration features. At least one LAN group must be defined before implementing advanced LAN configuration features.

### Security Menu

Security menu allows you to configure security tools like IP Filters.

### Status Menu

The Status menu provides the status for different connections or interfaces.

### Help Menu

The Help menu provides documentation about various router features.

## Chapter 3: Basic Menu

The Basic menu includes Home, Quick Start, LAN Configuration and Diagnostics.

Save Settings

Restart Router

Basic

Advanced

Security

Status

Help

Basic

Home

Quick Start

LAN Configuration

Diagnostics

Basic Home

Connection Information

DSL

UP

Downstream / Upstream (Kbps)

23278/1138

Internet

Connected

Connected Time

0hr 0min 23sec

Connection Type

PPPoA

Username

IP Address

192.168.35.8

Default Gateway

192.168.35.1

Primary DNS

192.168.2.1

Secondary DNS

165.21.100.88

Disconnect

Router Information

System Uptime

1 hours 46 minutes

Model

AT-AR256E v3

Firmware Version

119.12a.1-006

Ethernet MAC address

00:30:0A:96:D4:52

DSL MAC address

00:30:0A:96:D4:53

NAT

Enabled

Firewall

Enabled

Local Network

LAN IP Address

192.168.1.1

DHCP

Enabled

DHCP Range

192.168.1.2 - 192.168.1.254

Ethernet

Connected

Figure 4: Basic Home menu

### Home

The Home page provides a one-page summary about the Connection Information, Router Information and Local Network settings.

#### Connection Information

The Connection Information page gives you an idea about the status of your Internet connection. This page includes a Connect/Disconnect button. When clicked, the router makes an attempt to connect to the Internet using the parameters saved in the router.

#### Router Information

This page provides all the necessary information to determine the firmware version and Ethernet MAC Address.

#### Local Network

The Local Network page displays the current IP address of the router. It also provides the Ethernet status.

### Quick Start

Please refer to [Using Quick Start](#)

## LAN Configuration

LAN Configuration displays the current IP address assigned to the router. When you want to access the router, use the stated IP Address.

The screenshot shows the 'LAN Group 1 Configuration' page in the Allied Telesis web interface. The interface has a top navigation bar with 'Save Settings', 'Restart Router', and tabs for 'Basic', 'Advanced', 'Security', 'Status', and 'Help'. A left sidebar contains the 'Allied Telesis' logo and a menu with 'Basic', 'Home', 'Quick Start', 'LAN Configuration', and 'Diagnostics'. The main content area is titled 'LAN Group 1 Configuration' and contains the following fields and options:

- IP Address: 192.168.1.1
- Netmask: 255.255.255.0
- Default Gateway: (empty)
- Host Name: AT-AR256Ev3
- Domain: AlliedTelesis
- ☒ Enable DHCP Server ☐ Assign ISP DNS, SNTP
- Start IP: 192.168.1.2
- End IP: 192.168.1.254
- Lease Time: 3600 Seconds
- ☐ Enable DHCP Relay
- Relay IP: 20.0.0.3
- ☐ Server and Relay Off

At the bottom right of the configuration area are 'Apply' and 'Cancel' buttons.

Figure 5: LAN Configuration



## Diagnostics

Ping test is used for investigating the connection to another network device which is connected to your current device.

Full Modem Test is used for investigating whether the router is properly connected to the WAN. This test may take a few seconds to complete. To perform the test, select your connection from the list then press the Test button. Before running this test, make sure you have a valid DSL connection.

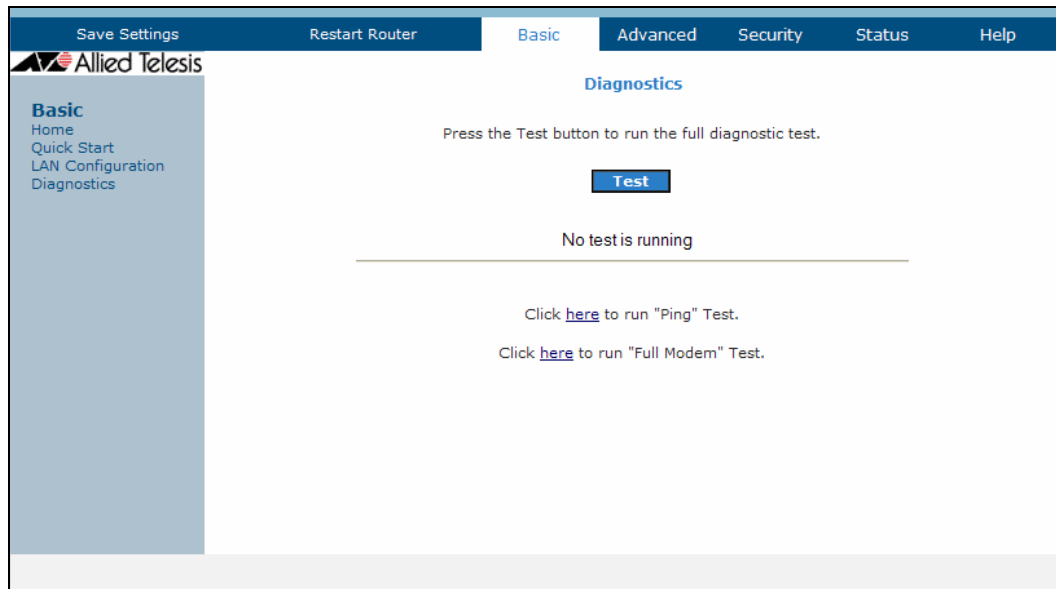


Figure 6: DSL Modem Test

### To run Modem Test:

1. Select the **Basic** menu then click **Diagnostics**. This opens the Full **Modem Test** page.
2. Click **Test**. The test results will appear after running the Modem Test.

## Chapter 4: Advanced Menu

This menu allows advanced configuration options for your router.

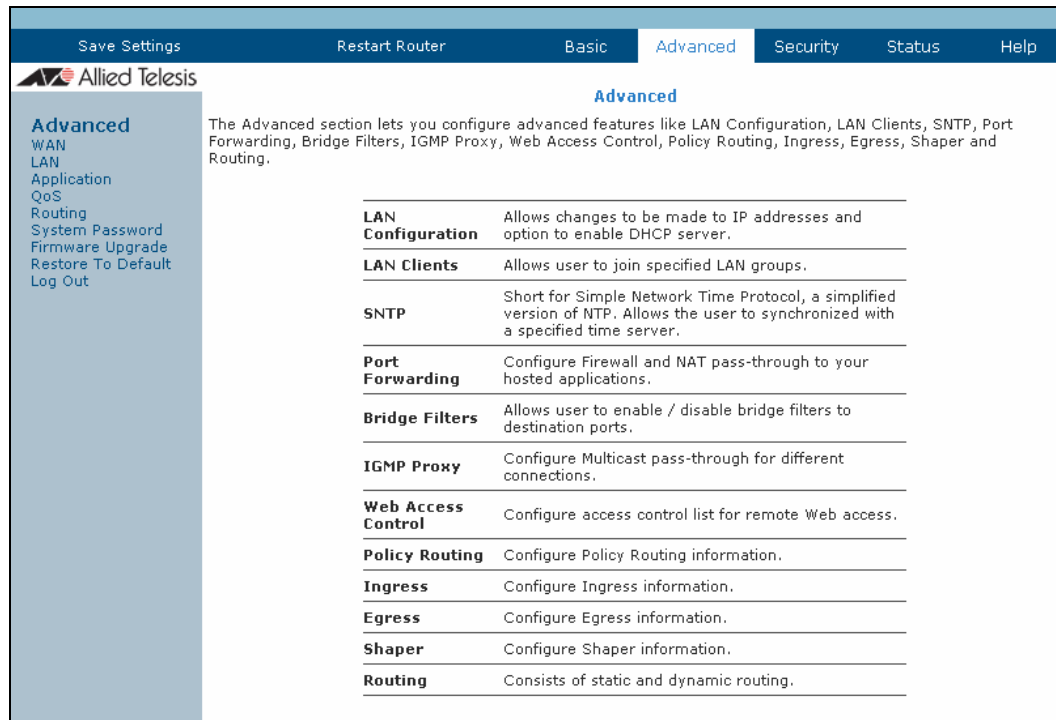


Figure 7: Advanced menu

## WAN

Wide Area Network refers to the configurations you perform to establish an Internet connection. There are several types of WAN connections that require different settings. Wide Area Network (WAN) is also referred to as the broadband connection. Connection settings differ for every service provider. Most of the configuration you perform is for the WAN connection.

### New Connection

Your router supports the creation of new connections. If you have multiple virtual connections, you may need to utilize the static routing capabilities of the modem to pass data correctly.

WAN connections types include:

- PPPoE Connection
- PPPoA Connection
- Static Connection
- DHCP Connection
- Bridge Connection

### PPPoE Connection

PPP or Point-to-Point Protocol, is a method of establishing a network connection/session between network hosts. PPPoE is a protocol for encapsulating PPP frames in Ethernet frames and is described in RFC 2516. PPPoE provides the ability to connect to a network of hosts over a simple bridging access device to a remote access concentrator. With this model, each router uses its own PPP stack. Access control, billing and type of service control can all be done on a per-user rather than per-site basis.

**PPPoE Connection Setup**

Name:  Type: **PPPoE** Sharing: **Disable**

Options: ☒ NAT ☒ Firewall VLAN ID:  Priority Bits:

**PPP Settings**

Encapsulation: ☒ LLC ☐ VC

Username:

Password:

Static IP Address:  ☐

Idle Timeout:  secs

Keep Alive:  min

Authentication: ☒ Auto ☐ CHAP ☐ PAP

MTU:  bytes

On Demand: ☐ Default Gateway: ☒

Enforce MTU: ☒ Debug: ☐

PPP Unnumbered: ☐ Valid Rx: ☐

Host Trigger: ☐ **Configure**

**Connect** **Disconnect**

**Apply** **Delete** **Cancel**

**PVC Settings**

PVC: **New**

VPI:

VCI:

QoS: **UBR**

PCR:  cps

SCR:  cps

MBS:  cells

CDVT:  usecs

Auto PVC: ☐

Figure 8: New PPPoE Connection Setup

### PPPoA Connection

PPPoA is also known as RFC 2364. It is a method of encapsulating PPP packets in ATM cells that are carried over the DSL connection. PPP or Point-to-Point Protocol, is a method of establishing a network connection/session between network hosts. It usually provides a mechanism for authenticating users. Logical Link Control (LLC) and Virtual Circuit (VC) are two different methods of encapsulating the PPP packet. Contact your service provider to determine which encapsulation is being used on your Internet connection.

**PPPoA Connection Setup**

Name:  Type: **PPPoA** Sharing: **Disable**

Options: ☒ NAT ☒ Firewall VLAN ID:  Priority Bits:

**PPP Settings**

Encapsulation: ☒ LLC ☐ VC

Username:

Password:

Static IP Address:  ☐

Idle Timeout:  secs

Keep Alive:  min

Authentication: ☒ Auto ☐ CHAP ☐ PAP

MTU:  bytes

On Demand: ☐ Default Gateway: ☒

Debug: ☐

Valid Rx: ☐

Host Trigger: ☐ **Configure**

**Connect** **Disconnect**

**Apply** **Delete** **Cancel**

**PVC Settings**

PVC: **New**

VPI:

VCI:

QoS: **UBR**

PCR:  cps

SCR:  cps

MBS:  cells

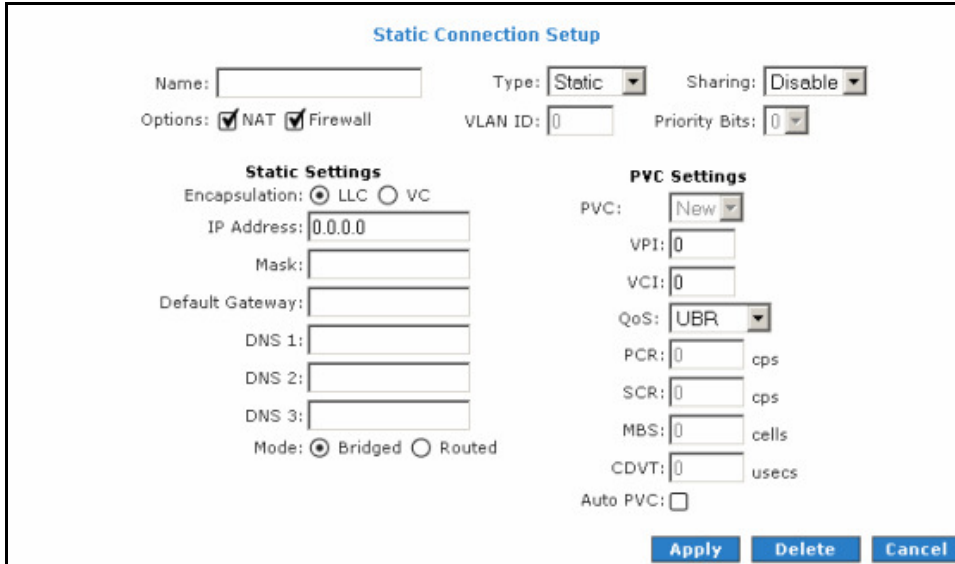
CDVT:  usecs

Auto PVC: ☐

Figure 9: New PPPoA Connection Setup

### Static Connection

Static connection type is used whenever a known static IP address is assigned to the router. Additional addressing information such as the subnet mask and the default gateway must also be specified. Up to three Domain Name Server (DNS) addresses can be identified. These servers resolve the name of the computer to the IP address mapped to it and thus enable you to access other web servers by typing the symbolic name (host name).



**Static Connection Setup**

Name:  Type: **Static** Sharing: **Disable**

Options: ☒ NAT ☒ Firewall VLAN ID:  Priority Bits:

**Static Settings**

Encapsulation: ☒ LLC ☐ VC

IP Address:

Mask:

Default Gateway:

DNS 1:

DNS 2:

DNS 3:

Mode: ☒ Bridged ☐ Routed

**PVC Settings**

PVC: **New**

VPI:

VCI:

QoS: **UBR**

PCR:  cps

SCR:  cps

MBS:  cells

CDVT:  usecs

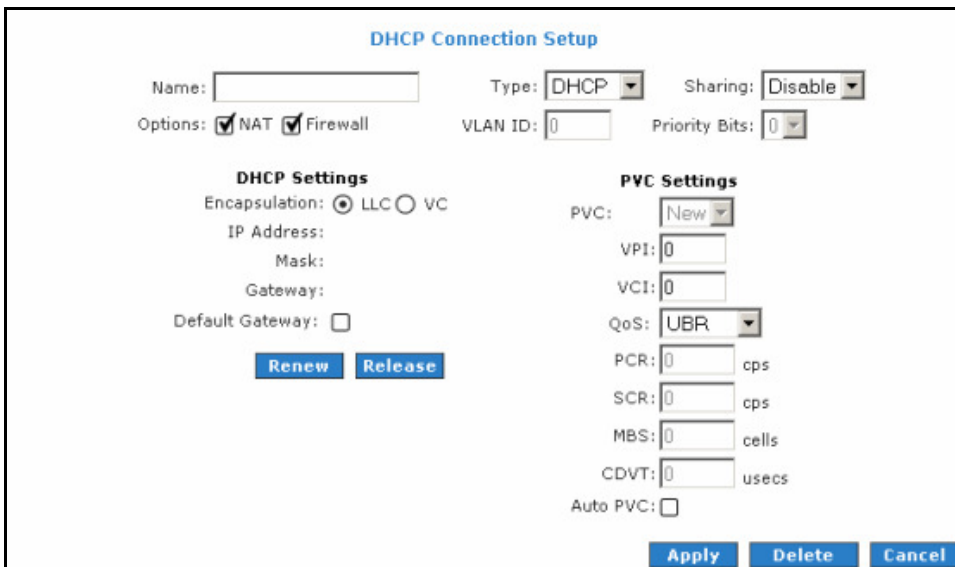
Auto PVC: ☐

**Apply Delete Cancel**

**Figure 10: New Static Connection Setup**

### DHCP Connection

Dynamic Host Configuration Protocol allows the router to automatically obtain a IP address from the server. This option is commonly used when the IP is dynamically assigned and is not known prior to assignment.



**DHCP Connection Setup**

Name:  Type: **DHCP** Sharing: **Disable**

Options: ☒ NAT ☒ Firewall VLAN ID:  Priority Bits:

**DHCP Settings**

Encapsulation: ☒ LLC ☐ VC

IP Address:

Mask:

Gateway:

Default Gateway: ☐

**Renew Release**

**PVC Settings**

PVC: **New**

VPI:

VCI:

QoS: **UBR**

PCR:  cps

SCR:  cps

MBS:  cells

CDVT:  usecs

Auto PVC: ☐

**Apply Delete Cancel**

**Figure 11: New DHCP Connection Setup**

## Bridge Connection

A pure bridged connection does not assign any IP address to the WAN interface. NAT and firewall rules are not enabled. This connection method makes the router act as a bridge for passing packets between the WAN interface and the LAN interface.

The screenshot displays the 'Bridged Connection Setup' window. At the top, the title 'Bridged Connection Setup' is centered. Below the title, there are three fields: 'Name:' followed by an empty text box, 'Type:' with a dropdown menu set to 'Bridge', and 'Sharing:' with a dropdown menu set to 'Disable'. Below these are 'Options:', 'VLAN ID:' with a text box containing '0', and 'Priority Bits:' with a dropdown menu set to '0'. The window is divided into two main sections: 'Bridge Settings' on the left and 'PVC Settings' on the right. Under 'Bridge Settings', there is 'Encapsulation:' with radio buttons for 'LLC' (selected) and 'VC', and 'Select LAN:' with a dropdown menu set to 'LAN group 1'. Under 'PVC Settings', there is 'PVC:' with a dropdown menu set to 'New', followed by 'VPI:' with a text box containing '0', 'VCI:' with a text box containing '0', 'QoS:' with a dropdown menu set to 'UBR', 'PCR:' with a text box containing '0' and 'cps' next to it, 'SCR:' with a text box containing '0' and 'cps' next to it, 'MBS:' with a text box containing '0' and 'cells' next to it, 'CDVT:' with a text box containing '0' and 'usecs' next to it, and 'Auto PVC:' with an unchecked checkbox. At the bottom right, there are three buttons: 'Apply', 'Delete', and 'Cancel'.

**Figure 12: New Bridge Connection Setup**

## ADSL Modulation

ADSL Modulation allows you to select any combination of DSL training modes. Leave the default values if you are unsure or the service provider did not provide this information. In most cases, this page should not be modified.

**Modem Setup**  
Select the modulation type.

☐ NO\_MODE  
☒ ADSL\_G.dmt  
☒ ADSL\_G.lite  
☒ ADSL\_G.dmt.bis  
☒ ADSL\_G.dmt.bis\_DELT  
☒ ADSL\_2plus  
☒ ADSL\_2plus\_DELT  
☒ ADSL\_re-adsl  
☒ ADSL\_re-adsl\_DELT  
☒ ADSL\_ANSI\_T1.413  
☒ MULTI\_MODE  
☐ ADSL\_G.dmt.bis\_AnXI  
☐ ADSL\_G.dmt.bis\_AnXJ  
☒ ADSL\_G.dmt.bis\_AnXM  
☐ ADSL\_2plus\_AnXI  
☐ ADSL\_2plus\_AnXJ  
☒ ADSL\_2plus\_AnXM  
☐ G.shdsl  
☐ IDSL  
☐ HDSL  
☐ SDSL  
☐ VDSL

**Apply** **Cancel**

Figure 13: ADSL Modulation

## Connection Scan

This feature helps users to detect the PVC settings provided by the service provider. Before the router can begin scanning the connection, the telephone line has to be plugged into the router.

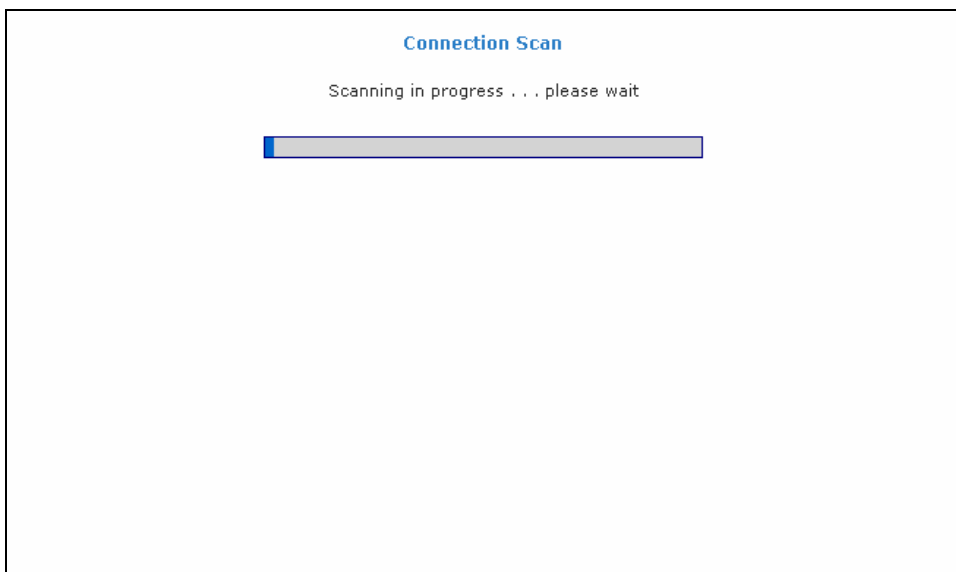


Figure 14: Connection Scan

### To perform connections scan:

1. Select the **Basic** menu.
2. Select Automatic
3. Click **Next**.
4. Select the appropriate settings and proceed with the login information.
5. Click **Connect**.

## LAN

The router is preconfigured to automatically provide IP addresses to all the computers in the Local Area Network (LAN). Your router allows you to create and configure LAN groups.

### LAN Configuration

Your router's default IP address and subnet mask are 192.168.1.1 and 255.255.255.0, respectively. This subnet mask allows the router to support 254 users. If you want to support more users, you need to edit the subnet mask but remember that the DHCP server is defaulted to only give out 254 IP addresses. If you change your gateways' IP address and you have DHCP enabled, the DHCP configuration must reside within the same subnet. The default gateway is the routing device used to forward all traffic that is not addressed to a station within the local subnet. Your ISP will provide you with the default gateway Address.

Figure 15: LAN Configuration

#### To configure the LAN groupings:

1. Select the **Advanced** menu.
2. Select LAN > LAN Configuration.
3. Select **ETHERNET** in **LAN group 1** then click **< Remove**. No packets will be sent to the ETHERNET interface because it does not belong to any LAN group.
4. Select **ETHERNET** from **Interfaces** then click **Add >** under **LAN group 2**. Just like in LAN group 1, **Configure** will appear in **LAN group 2** to allow the definition of additional configurations.
5. To temporarily activate the settings, click **Apply**.
6. To make changes permanent, click **Save Settings**.





## LAN Group Configuration

LAN Group Configuration allows you to configure settings for each LAN group. Notice that you can also view the status of advanced services that can be applied to a LAN group. Green indicates that the service is enabled, while red indicates that the service is disabled.

Figure 16: LAN Group Configuration


Category	Field	Description
<b>Unmanaged</b>		Unmanaged is a state when the LAN group is not configured and no IP address has been assigned to the bridge.
<b>Obtain an IP address automatically</b>		When this function is enabled, your router acts like a client and requests a IP address from the DHCP server on the LAN side.
	IP Address	You can retrieve/renew a IP address from the DHCP server using the Release and Renew buttons.
	Netmask	The subnet mask of your router.
<b>PPP IP Address</b>		Enables/disables PPP unnumbered feature.
	IP Address	The IP address should be different but within the same subnet as the WAN-side IP address.
<b>Use the following Static IP address</b>		This field enables you to change the IP address of the router.
	IP Address	The default IP address of the router (as shown) is 192.168.1.1.
	Netmask	The default subnet mask of your router is 255.255.255.0. This subnet allows the router to support 254 users. If you want to support a larger number of users, you can change the subnet mask.
	Default Gateway	The default gateway is the routing device used to forward all traffic that is not addressed to a station within the local subnet. Your ISP provides you with the IP address of the default gateway.
	Host Name	The host name is used in conjunction with the domain name to uniquely identify the router. It can be any alphanumeric word that does not contain spaces.

Category	Field	Description
	Domain	The domain name is used in conjunction with the host name to uniquely identify the router. To access the web pages of the router you can type 192.168.1.1 (the IP address) or AlliedTelesis.ATI (Host Name.Domain).
<b>Enable DHCP Server</b>		Enables/disables DHCP. By default, your router has the DHCP server (LAN side) enabled. If you already have a DHCP server running on your network, you must disable one of the two DHCP servers.
	Assign ISP DNS, SNTP	Enable/disables the Assign ISP DNS, SNTP feature when the DHCP server of your router has been enabled. To learn more, please refer to <a href="#">Assign ISP DNS, SNTP</a> .
	Start IP	The Start IP Address is where the DHCP server starts issuing IP addresses. This value must be greater than the IP address value of the router. For example, if the IP address of the router is 192.168.1.1 (default) then the starting IP address must be 192.168.1.2 (or higher).  <i>If you change the start and/or end values, make sure the values are still within the same subnet as the router. In other words, if the IP address of the router is 192.168.1.1 (default) and you change the DHCP start/end IP addresses to be 192.168.1.2/192.168.1.100, you cannot communicate with the router if your host has DHCP enabled.</i>
	End IP	The End IP Address is where the DHCP server stops issuing IP addresses. The ending address cannot exceed a subnet limit of 254; hence, the max value for the default gateway is 192.168.1.254. If the DHCP server runs out of DHCP addresses, users do not get access to network resources. If this happens, you can increase the Ending IP address (to the limit of 254) or reduce the lease time.  <i>If you change the start and/or end values, make sure the values are still within the same subnet as the IP address of the router. In other words, if the IP address of the router is 192.168.1.1 (default) and you change the DHCP start/end IP addresses to be 192.168.1.2/192.168.1.100, you cannot communicate with the router if your host has DHCP enabled.</i>
	Lease Time	The Lease Time is the amount of time that a network user is allowed to maintain a network connection to the router using the current dynamic IP address. At the end of the Lease Time, the lease is either renewed or the DHCP server issues a new IP. The amount of time is in units of seconds. The default value is 3600 seconds (1 hour). The maximum value is 999999 seconds (About 278 hours).
<b>Enable DHCP Relay</b>		In addition to the DHCP server feature, the router supports the DHCP relay function. When the router is configured as DHCP server, it assigns the IP addresses to the LAN clients. When the gateway is configured as DHCP relay, it is responsible for forwarding the requests and responses negotiated between the DHCP clients and the server.
	Relay IP	The IP address of the DHCP relay server.
<b>Server and Relay Off</b>		When the DHCP server and relay functions are turned off, the network administrator must carefully configure the IP address, Subnet Mask, and DNS settings of every host on your network. Do not assign the same IP address to more than one host. Also, your router must reside on the same subnet as all the other hosts.

### Assign ISP DNS, SNTP

When you enable the DHCP server, the router dynamically assigns IP addresses to computers in the local network. The router provides its own LAN IP address (192.168.1.1) as both the gateway and the DNS server.

The router has a choice of advertising its own IP address (192.168.1.1) as the DNS server or providing the DNS that was received from the WAN. This can be configured by enabling/disabling **Assign ISP DNS SNTP** on the **LAN Group Configuration** page.

	ISP DNS, SNTP only applies when the DHCP server is enabled on the LAN Group Configuration page
---	--

## LAN Clients

LAN Clients allows you to view and add computers in a LAN group. Each computer either has a dynamic or static (manually-configured) IP address.

You can add a static IP address (belonging to the router's LAN subnet) using the LAN Clients page. Any existing static entry falling within the DHCP server's range can be deleted.

Save Settings Restart Router Basic **Advanced** Security Status Help

Allied Telesis

**Advanced**  
WAN  
LAN  
Application  
QoS  
Routing  
System Password  
Firmware Upgrade  
Restore To Default

**LAN Clients**

To add a LAN Client, Enter IP Address and Hostname, then click Apply.

Select LAN Connection: LAN group 1

Enter IP Address:

Hostname:

MAC Address:

**Dynamic Addresses**

Reserve	IP Address	Hostname	MAC	Type
<input type="checkbox"/>	192.168.1.2	ProductSharePC	00:11:43:b7:e7:f2	Dynamic

Apply Cancel

Figure 17: LAN Clients

### To add LAN Clients:

1. Select **Advanced** menu.
2. Select **LAN > LAN Clients**. This opens the **LAN Clients** page.
3. Select a LAN Connection and enter IP Address, Hostname and MAC Address.
4. Click **Apply**.
5. You can convert the dynamic into a static entry by clicking **Reserve**, and then click **Apply**.
6. To temporarily implement the settings, click **Apply**.
7. To make changes permanent, click **Save Settings**.

## Applications

Applications include:

- Universal Plug and Play (UPnP)
- Simple Network Time Protocol (SNTP)
- Internet Group Management Protocol (IGMP) Proxy
- TR-068 WAN Access
- DNS Proxy
- Dynamic DNS Client
- Port Forwarding
- Bridge Filters
- Web Access Control

## Universal Plug and Play (UPnP)

**Universal Plug and Play (UPnP)** is a set of computer network protocols allow devices to connect seamlessly and to simplify the implementation of networks in the home (data sharing, communications, and entertainment) and corporate environments.

The screenshot shows the 'Advanced' tab of the router's configuration page. The 'UPnP' section is active, displaying the instruction: 'To enable UPnP, check the Enable UPnP box and select a connection below.' There is an unchecked checkbox labeled 'Enable UPnP'. Below it, two dropdown menus are shown: 'WAN Connection' set to 'PPPoA' and 'LAN Connection' set to 'LAN group 1'. At the bottom right are 'Apply' and 'Cancel' buttons. A sidebar on the left lists various configuration options under the 'Advanced' heading.

Figure 18: UPnP

To enable UPnP check the 'enable UPNP' checkbox, then Apply.

## Simple Network Time Protocol

Simple Network Time Protocol (SNTP) is a protocol used to synchronize the system time to the public SNTP servers. It uses the UDP protocol on port 123 to communicate between clients and servers.

The screenshot shows the 'SNTP' configuration page. The instruction reads: 'To enable SNTP, check the Enable SNTP box and enter a time server.' There is an unchecked checkbox labeled 'Enable SNTP'. Below it are three text input fields for 'Primary SNTP Server', 'Secondary SNTP Server', and 'Tertiary SNTP Server', each containing '0.0.0.0'. There are also input fields for 'Timeout' (5) with a 'Secs' label, 'Polling Interval' (30) with a 'Mins' label, and 'Retry Count' (2). A dropdown menu for 'Time Zone' is set to '(GMT-12:00) International Date Line West'. A 'Day Light' checkbox is present and unchecked. 'Apply' and 'Cancel' buttons are at the bottom right.

Figure 19: SNTP

### To enable SNTP:

1. Check Enable SNTP.
2. Configure the following fields:
  - **Primary SNTP Server** The IP address or host name of the primary SNTP server. This can be provided by the ISP or defined by a user.

- **Secondary SNTP Server** The IP address or host name of the secondary SNTP server. This can be provided by the ISP or defined by a user.
  - **Tertiary SNTP Server** The IP address or host name of the tertiary SNTP server. This can be provided by the ISP or defined by a user.
  - **Timeout** If the router failed to connect to a SNTP server within the Timeout period, it retries the connection.
  - **Polling Interval** The amount of time between a successful connection with a SNTP server and a new attempt to connect to a SNTP server.
  - **Retry Count** The number of times the router tries to connect to a SNTP server before it tries to connect to the next server in line.
  - **Time Zone** The time zone in which the router resides.
  - **Day Light** Select this option to enable/disable Daylight Saving Time (DST). DST is not automatically enabled or disabled. You need to manually enable and disable it.
3. Click **Apply** to temporarily apply the settings.
  4. To make changes permanent, click **Save Settings**.

## IGMP Proxy

IP hosts use Internet Group Management Protocol (IGMP) to report their multicast group memberships to neighboring routers. Similarly, multicast routers use IGMP to discover which of their hosts belong to multicast groups. Your router supports IGMP proxy that handles IGMP messages. When enabled, your router acts as a proxy for a LAN host making requests to join and leave multicast groups, or a multicast router sending multicast packets to multicast groups on the WAN side.

**IGMP Proxy**

IGMP Proxy could be enabled on WAN and LAN connections.

☐ **Enable IGMP Proxy**

**Interface**      **Upstream/Downstream/Ignore**

quickstart      Ignore

LAN group 1      Ignore

**Apply**    **Cancel**

**Figure 20: IGMP Proxy**

Multicasting is a form of limited broadcast. UDP is used to send datagram's to all hosts that belong to what is called a Host Group. A host group is a set of one or more hosts identified by a single IP destination address. The following statements apply to host groups:

- Anyone can join or leave a host group at will.
- There are no restrictions on a host's location.
- There are no restrictions on the number of members that may belong to a host group.
- A host may belong to multiple host groups.
- Non-group members may send UDP datagrams to the host group.

Multicasting is useful when the same data needs to be sent to more than one device. For instance, if one device is responsible for acquiring data that many other devices need then multicasting is a natural fit. Note

that using multicasting as opposed to sending the same data to individual devices uses less network bandwidth. The multicast feature also enables you to receive multicast video streams from multicast servers. The IGMP Proxy page allows you to enable multicast on available WAN and LAN connections. You can configure the WAN or LAN interface as one of the following:

- **Upstream** The interface that IGMP requests from hosts are sent to the multicast router.
- **Downstream** The interface data from the multicast router are sent to hosts in the multicast group database.
- **Ignore** No IGMP request nor data multicast is being forwarded.

You can perform one of the two options:

- Configure one or more WAN interface as the upstream interface.
- Configure one or more LAN interface as the upstream interface.

#### To configure the IGMP Proxy:

1. Select **Advanced**.
2. Select Application > IGMP Proxy.
3. Configure the following interfaces:
  - Quickstart
  - LAN group I
4. Click **Apply** to temporarily apply the settings.
5. To make changes permanent, click **Save Settings**.

## TR-068 WAN Access

The TR-068 WAN Access page enables you to give temporary permission to someone (such as technical support staff) to be able to access your router from the WAN side. From the moment the account is enabled, the user is expected to log in within 20 minutes; otherwise, the account expires. Once the user has logged in, if the session remains inactive for more than 20 minutes, the user will be logged out and the account expires.

**Enable WAN Access Update**

To Enable Webpage Update from WAN side

WAN Update: ☐

WAN Access: ☐

User Name:

Password:

Port:

**Figure 21: Enable WAN Access Update**

#### To create a temporary user account for remote access:

1. Select the **Advanced** menu.
2. Select Application > TR-068 WAN Access.
3. Select WAN Update.

4. Select WAN Access.
5. Enter a username and password in the **User Name** and **Password** fields.
6. Enter a port number in the **Port** field (for example, 51003).  
To access your router remotely, enter the following URL:
  - http(s)://10.10.10.5:51003
  - **Syntax:** http(s)://WAN IP of router: Port Number
7. Click **Apply** to temporarily apply the settings.
8. To make changes permanent, click **Save Settings**.

## DNS Proxy

DNS Proxy determines the primary Domain Name Server and secondary DNS to be used.

Figure 22: DNS Proxy

### To select the DNS Server Priority:

1. Select **Advanced**.
2. Select **Application > DNS Proxy**.
3. Select the DNS Server Priority.
  - Only Auto Discovered DNS Servers
  - Only User Configured DNS Servers
  - Auto Discovered then User Configured
  - User Configured then Auto Discovered
4. Click **Apply** to temporarily apply settings.
5. To make changes permanent, click **Save Settings**.

## Dynamic DNS Client

Dynamic DNS allows the user to register with a Dynamic DNS Provider. The Dynamic DNS will be linked with the WAN IP of the router even after the ISP update the WAN IP to another IP address. It can be useful in web hosting and FTP services.



The User Name/Password entered should be similar to the User Name/Password you have specified during the registration of the DNS hostname.

### To enable Dynamic DNS:

1. Select Advanced.
2. Select Application > Dynamic DNS Client.
3. Configure the following fields:
  - Connection
  - DDNS Server
  - DDNS Client
  - User Name
  - Password
  - Domain Name
4. Click Apply to temporarily apply the settings.
5. To make changes permanent, click Save Settings.

The screenshot shows the 'Dynamic DNS Client' configuration page. At the top, there are tabs: 'Save Settings', 'Restart Router', 'Basic', 'Advanced' (selected), 'Security', 'Status', and 'Help'. Below the tabs is the 'Allied Telesis' logo and a sidebar menu with options: 'Advanced' (selected), 'WAN', 'LAN', 'Application', 'QoS', 'Routing', 'System Password', 'Firmware Upgrade', and 'Restore To Default'. The main content area is titled 'Dynamic DNS Client' and contains the following fields:
 

- DDNS Server: A dropdown menu set to 'dyndns'.
- DDNS Client: A checkbox that is checked.
- User Name: A text input field containing 'username'.
- Password: A text input field with masked characters (dots).
- Domain Name: A text input field containing 'domain.dyndns.org'.

Figure 23: Dynamic DNS Client

## Port Forwarding

Port forwarding (or virtual server) allows you to direct incoming traffic to specific LAN hosts based on a protocol port number and protocol. Using the Port Forwarding page, you can provide local services (for example, web hosting) for people on the Internet or play Internet games. Port forwarding is configurable per LAN group.

The screenshot shows the 'Port Forwarding' configuration page. At the top, there are tabs: 'WAN Connection', 'Select LAN Group', 'LAN IP', 'New IP', 'DMZ', and 'Custom Port Forwarding'. The 'WAN Connection' dropdown is set to 'quickstart'. The 'Select LAN Group' dropdown is set to 'LAN group 1'. The 'LAN IP' dropdown is set to '192.168.1.2'. There is an unchecked checkbox for 'Allow Incoming Ping'. Below these fields are buttons for 'New IP', 'DMZ', and 'Custom Port Forwarding'. The main content area is divided into two sections: 'Available Rules' and 'Applied Rules'. The 'Available Rules' section has a 'Category' list on the left (Games, VPN, Audio/Video, Apps, Servers, User) and a list of rules on the right: 'Alien vs Predator', 'Asheron's Call', 'Dark Rein 2', 'Delta Force', 'Doom', 'Dune 2000', 'DirectX (7.8) Games', 'EliteForce', 'EverQuest', and 'Fighter Ace II'. There are 'Add >' and '< Remove' buttons between the two lists. At the bottom right, there are 'Apply' and 'Cancel' buttons.

Figure 24: Port Forwarding



A database of predefined port forwarding rules allows you to apply one or more rules to one or more members of a defined LAN group. You can view the rules associated with a predefined category and add the available rules for a given category. You can also create, edit or delete your own port forwarding rules.

**To configure port forwarding:**

1. Select **Advanced**.
2. Select **Application > Port Forwarding**.
3. Select **WAN Connection**, **LAN Group** and **LAN IP**. If the desired LAN IP is not available in the **LAN IP** drop-down menu, you can add it using the **LAN Client** page, which is accessed by clicking **New IP**.
4. Select the available rules for a given category and click **Add** to apply the rule for this category. If a rule is not in the list, you can create your own rule in the **User** category. Select **User**, and then click **New**.
5. The Rule Management page opens for you to create new rules. Enter **Rule Name**, **Protocol**, **Port Start**, **Port End** and **Port Map** then click **Apply**.
6. Continue to add rules as they apply from each category.
7. Click **Apply** to temporarily activate the settings.
8. To make changes permanent, click **Save Settings**.

### DMZ Settings

Setting a host on your local network as demilitarized zone (DMZ) forwards any network traffic that is not redirected to another host via the Port Forwarding feature to the IP address of the host. This opens the access to the DMZ host from the Internet. This function is disabled by default. By enabling DMZ, you add an extra layer of security protection for hosts behind the firewall.

**To enable DMZ Settings:**

1. On the **Port Forwarding** page, select **Enable DMZ**. This opens the DMZ Settings page.
2. Select the **WAN Connection**, **LAN Group** and **LAN IP Address**.
3. Click **Apply** to temporarily apply the settings.
4. To make changes permanent, click **Save Settings**.

### Custom Port Forwarding

The Custom Port Forwarding page allows you to create up to 15 custom Port Forwarding entries to support specific services or applications, such as concurrent NAT/NAPT operation.

## Bridge Filters

The Bridge Filters allows you to enable, add, edit or delete the filter rules. When bridge filtering is enabled, each frame is examined against every defined filter rule in sequence. When a match is found, the appropriate filtering action (allow or deny) is performed. Up to 20 filter rules are supported with bridge filtering.

**Bridge Filters**

☐ Enable Bridge Filters

☐ Enable Bridge Filter Management Interface

Select LAN: LAN group 1

Bridge Filter Management Interface: Ethernet

Src MAC	Src Port	Dest MAC	Dest Port	Protocol	Mode
00-00-00-00-00-00	ANY	00-00-00-00-00-00	ANY	PPPoE Session	Deny

Add

Edit	Src MAC	Src Port	Dest MAC	Dest Port	Protocol	Mode	Delete
------	---------	----------	----------	-----------	----------	------	--------

Apply Cancel

Figure 25: Bridge Filters

### To configure Bridge Filters:

1. Select **Advanced**.
2. Select **Application > Bridge Filters**. This opens the Bridge Filters page.
3. Select **Enable Bridge Filters**.
4. To add a rule, enter the source **MAC address**, **Destination MAC address** and **Protocol** with desired filtering type, then click **Add**.



You can also edit a rule that you created using the **Edit** checkbox. You can delete using **Delete**.

5. Click **Apply** to temporarily activate the settings.
6. To make changes permanent, click **Save Settings**.

## Web Access Control

The Web Access Control page allows you to access the router via the web from a remote location like your home or office.



Web Access Control

Enable: ☐

Choose a connection: quickstart

Remote Host IP: 0.0.0.0

Remote Netmask: 255.255.255.255

Redirect Port: 8080

Apply Cancel

Figure 26: Web Access Control

### To configure Web Access:

1. Select **Advanced** menu.
2. Select **Application > Web Access Control**.
3. Select **Enable**.
4. Select the connection used in **Choose a connection**.
5. Configure the following fields:
  - Remote Host IP
  - Remote Netmask
  - Redirect Port
6. Click **Apply** to temporarily activate the settings on the page. The WAN address is now added into the IP Access List. This allows you to access your router remotely.
7. To make changes permanent, click **Save Settings**.

## Quality of Service

Quality of Service allows network administrators to configure the routers to meet the real time requirements for voice and video.

Different networks use different QoS markings like:

- ToS network: ToS bits in the IP header
- VLAN network: priority bits in the VLAN header
- DSCP network: uses only 5 bits of the CoS
- WLAN: WLAN QoS header.

The QoS framework is supported on all the above domains. How do you make them talk to each other? How can you make sure the priority from one network is carried over to another network? Class of service (CoS) is introduced as the common language for the QoS mappings. When QoS is enabled, the router has full control over packets from the time they enter the router till they leave the router. This is how it works: The domain mapping (ToS bits, priority bits, etc.) of a packet needs to be translated to CoS when the packet enter the router and vice versa, the CoS of a packet needs to be translated back to the domain mapping when the packet leaves the router.

There are 6 types of CoS (in descending priority):

- CoS1
- CoS2
- CoS3
- CoS4
- CoS5
- CoS6

The rules are:

1. CoS1 has absolute priority and is used for Expedited Forwarding (EF) traffic. This is always serviced till completion.
2. CoS2-CoS5 is used for Assured Forwarding (AF) classes. They are serviced in a strict round robin manner using the following priority scheme:  
CoS2 > CoS3 > CoS4 > CoS5
3. CoS6 is for Best Effort (BE) traffic. This is only serviced when there is no other class of service. If QoS is not enabled on your router, all traffic will be treated as best effort.

There are some additional terms you should get familiarize with:

- Ingress: Packets arriving into the router from a WAN/LAN interface.
- Egress: Packets sent from the router to a WAN/LAN interface.
- Trusted mode: Honors the domain mapping (ToS byte, WME, WLAN user priority).
- Untrusted mode: Does not honor domain mapping. This is the default QoS setting.
- Traffic Conditioning Agreement (TCA): The TCA needs to be defined for each interface:
  - Ingress mappings (Domain => CoS)
  - Egress Mappings (CoS => Domain)
  - Untrusted mode (default)
- Shaper

## Egress

For packets going out of the router, the markings (CoS) need to be translated to the mappings understood by the network domains. The reverse CoS and domain mapping is configured using the Egress. To access **Egress**, select the **Advanced** menu then select **QoS > Egress**.

There are three Egress modes:

- No Egress mode
- Layer 2
- Layer 3

### No Egress

The default Egress page setting for all interfaces is No Egress. In this mode, the domain mappings of the packets are untouched.

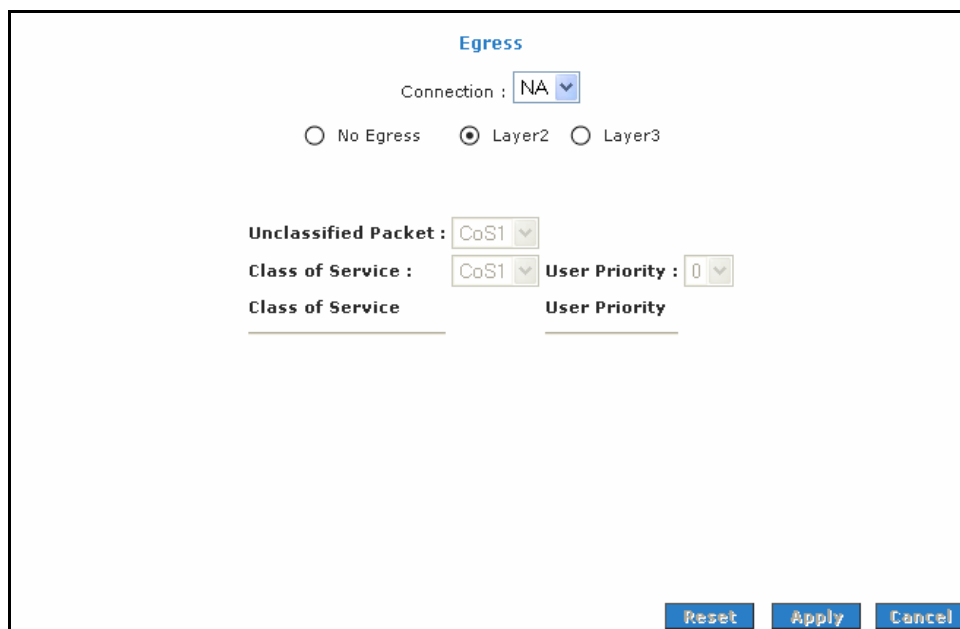


The screenshot shows the 'Egress' configuration window for the 'Ethernet1' connection. At the top, the title 'Egress' is displayed. Below it, the 'Connection' dropdown is set to 'Ethernet1'. There are three radio button options: 'No Egress' (which is selected), 'Layer2', and 'Layer3'. In the center of the window, the text 'No Egress TCA defined' is displayed. At the bottom right, there is a 'Cancel' button.

**Figure 27: Egress**

### Layer 2 Egress

The Egress Layer 2 page allows you to map the CoS of an outgoing packet to user priority bits, which is honored by the VLAN network. Again, this feature is only configurable on the WAN interface as VLAN is only supported on the WAN side in the current release.



The screenshot shows the 'Egress' configuration window for the 'NA' connection. At the top, the title 'Egress' is displayed. Below it, the 'Connection' dropdown is set to 'NA'. There are three radio button options: 'No Egress', 'Layer2' (which is selected), and 'Layer3'. Below the radio buttons, there are two rows of configuration options. The first row shows 'Unclassified Packet' set to 'CoS1' and 'Class of Service' set to 'CoS1'. The second row shows 'User Priority' set to '0'. Below these rows, there are labels 'Class of Service' and 'User Priority' with horizontal lines underneath them. At the bottom right, there are three buttons: 'Reset', 'Apply', and 'Cancel'.

**Figure 28: Layer 2 Egress**

Field	Description
<b>Interface</b>	Select the WAN interface to configure the QoS for outgoing packets; LAN interface cannot be selected as VLAN is currently supported on the WAN side only.
<b>Unclassified Packet</b>	Some locally generated packets might not have been classified and thus do not have a CoS value, such as PPP control packet and ARP packet. You can define the CoS for all unclassified outgoing packets on layer 2 using this field, which will then pick up the user priority bits based on the mapping rules you create. The selections are (in the order of descending priority): CoS1, CoS2, CoS3, CoS4, CoS5 and CoS6. The default value is CoS1 (recommended).
<b>Class of Service</b>	The selections are (in the order of descending priority): CoS1, CoS2, CoS3, CoS4, CoS5 and CoS6.
<b>User Priority</b>	The selections are 0, 1, 2, 3, 4, 5, 6 and 7.

### Layer 3 Egress

Egress Layer 3 enables you to map CoS to ToS so that the priority marking of outgoing packets can be carried over to the IP network.

**Egress**

Connection : Ethernet1

☐ No Egress
 ☐ Layer2
 ☒ Layer3

Default Non-IP: CoS1

Class of Service : CoS1 Translated Tos:

Class of Service
Translated TOS

Reset
Apply
Cancel

**Figure 29: Layer 3 Egress**

Field	Description
<b>Interface</b>	Select the WAN interface to configure the QoS for outgoing packets; LAN interface cannot be selected as VLAN is currently supported on the WAN side only.
<b>Default Non-IP</b>	Locally generated packets (such as ARP packets) do not have a CoS marking. You can define the CoS for all unclassified outgoing packets on layer 3 using this field. The selections are (in the order of descending priority): CoS1, CoS2, CoS3, CoS4, CoS5 and CoS6. The default value is CoS1 (recommended).
<b>Class of Service</b>	The selections are (in the order of descending priority): CoS1, CoS2, CoS3, CoS4, CoS5 and CoS6.
<b>Translated TOS</b>	The Type of Service field takes values from 1 to 255. The selections are 0, 1, 2, 3, 4, 5, 6 and 7.

### Ingress

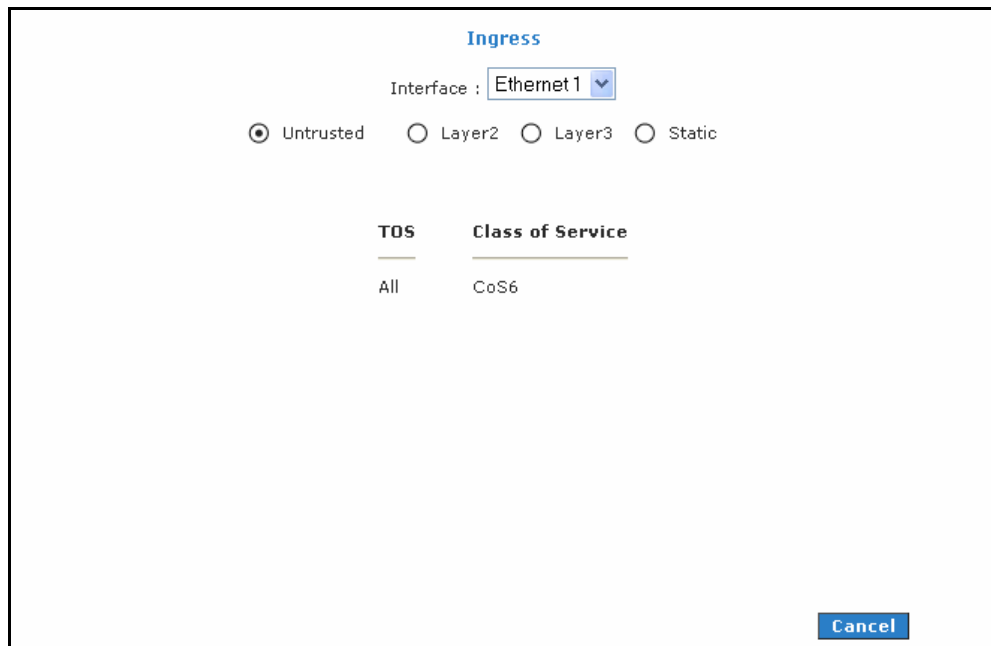
Ingress enables you to configure QoS for packets as soon as they come into the router. The domain mappings are converted to CoS (the common language) so that the priority marking is carried over.

There are four Ingress modes:

- Untrusted mode
- Layer 2
- Layer 3
- Static

### Untrusted Mode

Untrusted is the default Ingress page setting for all interfaces. In this mode, no domain mapping is honored in the router. All packets are treated as CoS6 (best effort).



The screenshot shows the 'Ingress' configuration page for the 'Ethernet1' interface. The 'Interface' dropdown is set to 'Ethernet1'. Below it, four radio buttons are present: 'Untrusted' (selected), 'Layer2', 'Layer3', and 'Static'. Underneath, there are two columns: 'TOS' and 'Class of Service'. The 'TOS' column has a value of 'All', and the 'Class of Service' column has a value of 'CoS6'. A 'Cancel' button is located in the bottom right corner.

TOS	Class of Service
All	CoS6

**Figure 30: Untrusted mode Ingress**

## Layer 2 Ingress

Layer 2 allows you to map an incoming packet with VLAN priority to CoS. This feature is only configurable on the WAN interface as VLAN is only supported on the WAN side in the current software release.

Figure 31: Layer 2 Ingress

Field	Description
Interface	Select the WAN interface here to configure the CoS for incoming traffic. Only WAN interface can be selected as VLAN is currently supported only on the WAN side.
Class of Service	The selections are (in the order of descending priority): CoS1, CoS2, CoS3, CoS4, CoS5 and CoS6.
User Priority	The selections are 0, 1, 2, 3, 4, 5, 6 and 7.

### To configure Ingress Layer 2:

1. Select **Advanced** menu.
2. Select **QoS > Ingress**.
3. Select the **quickstart** interface.
4. Select **Layer 2**.
5. Select **CoS1** in **Class of Service** and enter **5** in **Priority Bits**. Any packet with priority marking 5 is mapped to CoS1, the highest priority that is normally given to voice packets.
6. Click **Apply** to temporarily the settings.
7. Select **CoS2** in the **Class of Service** and **1** in **Priority Bits**. Any packet that has a priority bit of 1 is mapped to CoS2, which is the second highest priority. This is given to the high priority packets such as video.
8. Click **Apply** to temporarily activate the settings.
9. Repeat steps 5-7 to add more rules. Up to eight rules can be configured for each interface.
10. To make changes permanent, click **Save Settings**.



Any priority bits that have not been mapped to a CoS default to CoS6, the lowest priority. Any WAN interface that is not configured has the default Untrusted mode.



### Layer 3 Ingress


The Layer 3 page allows you to map ToS bits of incoming packets from the IP network to CoS for each WAN/LAN interface.

Figure 32: Layer 3 Ingress

Field	Description
<b>Interface</b>	For both WAN and LAN interfaces, you can configure QoS for layer 3 (IP) data traffic.
<b>Class of Service</b>	This CoS field allows you to map incoming layer 3 WAN/LAN packets to one of the following CoS (in the order of descending priority): CoS1, CoS2, CoS3, CoS4, CoS5 and CoS6.
<b>ToS</b>	The Type of Service field takes values from 0 to 255.
<b>Default Non-IP</b>	A static CoS can be assigned to all layer 3 incoming packets (per interface) that do not have a IP header, such as PPP control packets and ARP packets. The default is CoS1 (recommended).

#### To configure Ingress Layer 3:

11. Select **Advanced** menu.
12. Select **QoS > Ingress**.
13. Select the **quickstart** interface.
14. Select **Layer 3**.
15. Select **CoS1** in **Class of Service** and enter **22** in **Type of Service (ToS)**. Any incoming packet from LAN Group 1 (layer 3) with a ToS of 22 is mapped to CoS1, the highest priority, which is normally given to voice packets.
16. Leave the default value CoS1 in Default Non-IP. Any incoming packet from LAN Group 1 without a IP is mapped to CoS1, the highest priority.
17. Click **Apply** to temporarily activate the settings.
18. Repeat step 5-7 to add more rules to LAN Group 1. Up to 255 rules can be configured for each interface.
19. To make changes permanent, click **Save Settings**.

 Any priority bits that have not been mapped to a CoS default to CoS6, the lowest priority.  
Any WAN interface that is not configured has the default Untrusted mode.

### Static Ingress

The Ingress - Static page enables you to configure a static CoS for all packets received on a WAN or LAN interface.

The screenshot shows the 'Ingress' configuration page. At the top, the title 'Ingress' is displayed. Below it, the 'Interface' is set to 'Ethernet 1'. There are four radio buttons for selecting the mode: 'Untrusted', 'Layer2', 'Layer3', and 'Static'. The 'Static' radio button is selected. Below the radio buttons, the 'Class of Service' is set to 'CoS1'. At the bottom right, there are three buttons: 'Reset', 'Apply', and 'Cancel'.

Figure 33: Static

#### To configure Ingress Static:

1. Select **Advanced** menu.
2. Select **QoS > Ingress**.
3. Select the **quickstart** interface.
4. Select **Static**.
5. At the ETHERNET Interface. You are configuring QoS on this interface only. Any WAN/LAN interface that is not configured has the default Untrusted mode.
6. Select **CoS1** in **Class of Service**. All incoming traffic from the ETHERNET interface receives **CoS1**, the highest priority.
7. Click **Apply** to temporarily activate the settings.
8. To make changes permanent, click **Save Settings**.

### QoS Shaper Configuration

The QoS Shaper Configuration page is accessed by selecting Shaper on the Advanced page. Three shaper algorithms are supported:

- HTB
- Low Latency Queue Discipline
- PRIOWRR

**QoS Shaper Configuration**

Interface : Ethernet1

☐ **HTB Queue Discipline**      Max Rate:

☐ **Low Latency Queue Discipline**

CoS1 :  Kbits    CoS2 :  Kbits

CoS3 :  Kbits    CoS4 :  Kbits


CoS5 :  Kbits    CoS6 :  Kbits

☐ **PRIOWRR**

CoS2 :  %    CoS3 :  %    CoS4 :  %    CoS5 :  %    CoS6 :  %

Reset
Apply
Cancel

**Figure 34: QoS Shaper Configuration**

	Egress TCA is required if shaper is configured for that interface.
---	--

Field	Description
<b>Interface</b>	The selections are WAN/LAN interfaces except WLAN, which does not support Shaper feature. This field needs to be selected before shaper configuration.
<b>Max Rate</b>	This field is applicable for the HTB Queue Discipline and Low Latency Queue Discipline; both are rate-based shaping algorithms.
<b>HTB Queue Discipline</b>	The Hierarchical Token Bucket queue discipline is a rate-based shaping algorithm. This algorithm rate shapes the traffic of a class over a specific interface. All CoSx traffic use a specific rate to which data will be shaped. For example: If CoS1 is configured to 100Kbits then even if 300Kbits of CoS1 data is being transmitted to the interface, only 100Kbits will be sent out.
<b>Low Latency Queue Discipline</b>	This is similar to the above algorithm except that CoS1 is not rate limited. So in the example above CoS1 data is not rate limited to 100Kbits but instead all 300Kbits is transmitted. The side effect is that a misconfigured stream can potentially take all bandwidth.
<b>PRIOWRR</b>	This is a priority based weighted round robin algorithm operating on CoS2-CoS6. CoS1 queues have the highest priority and are not controlled by the WRR algorithm.

Of the three shaping algorithms available on the Shaper Configuration page, only one can be enabled at a time. An example of each configuration is given as follows.

### Example 1: HTB Queue Discipline Enabled

In the example below, HTB Queue Discipline is enabled. The PPPoE1 connection has a total of 300Kbits of bandwidth, of which 100Kbits is given to CoS1 and another 100Kbits is given to CoS2. When there is no CoS1 or CoS2 packet, CoS6 packets have the whole 300Kbits of bandwidth.

The screenshot shows the 'QoS Shaper Configuration' window. The 'Interface' is set to 'Ethernet1'. The 'HTB Queue Discipline' checkbox is checked, and the 'Max Rate' field is empty. The 'Low Latency Queue Discipline' and 'PRIOWRR' checkboxes are unchecked. Under HTB, there are input fields for CoS1 through CoS6, each followed by 'Kbits'. CoS1 and CoS2 are highlighted in blue. At the bottom, there are 'Reset', 'Apply', and 'Cancel' buttons.

Figure 35: HTB Queue Discipline enabled

### Example 2: Low Latency Queue Discipline Enabled

In this second example, Low Latency Queue Discipline is enabled. CoS1 is not rate controlled (hence the field is disabled). CoS2 takes 100Kbits when there is no CoS1 packet. CoS6 has 300Kbits when there is no CoS1 or CoS2 packets. This is similar to the HTB queue discipline as they are both rate-based algorithm, except that CoS1 is handled differently.

The screenshot shows the 'QoS Shaper Configuration' window. The 'Interface' is set to 'Ethernet1'. The 'HTB Queue Discipline' checkbox is unchecked, and the 'Max Rate' field is empty. The 'Low Latency Queue Discipline' checkbox is checked. Under Low Latency, there are input fields for CoS1 through CoS6, each followed by 'Kbits'. CoS1 is disabled (greyed out). At the bottom, there are 'Reset', 'Apply', and 'Cancel' buttons.

Figure 36: Low Latency Queue Discipline enabled

### Example 3: PRIOWRR Enabled

In this third example, PRIOWRR is enabled. Since PRIOWRR operates only on the number of packets being transmitted, the max rate field has been disabled. Only percentage can be assigned to the CoS2 - CoS6.

CoS1 is not rate controlled (hence the field is not displayed). When there is no CoS1 packet, CoS2, CoS3, CoS4 each has 10% and CoS6 has 70%. This is similarly to the Low Latency Queue discipline, except that one is packet-based and the other is rate-based.

**QoS Shaper Configuration**

Interface : Ethernet1

☐ HTB Queue Discipline      Max Rate:

☐ Low Latency Queue Discipline

CoS1 : Kbits      CoS2 : Kbits

CoS3 : Kbits      CoS4 : Kbits

CoS5 : Kbits      CoS6 : Kbits

☒ PRIOWRR

CoS2 : %      CoS3 : %      CoS4 : %      CoS5 : %      CoS6 : %

Reset    Apply    Cancel

**Figure 37: PRIOWRR enabled**

## Policy Routing Configuration

The Policy Routing Configuration enables you to configure policy routing and QoS.

**Policy Routing Configuration**

Ingress Interface : LAN group 1      Destination Interface : quickstart

DiffServ Code Point :      Class of Service : CoS1

Source IP :      Destination IP :      Mask :      Mask :

Protocol : TCP      tcp

Source Port :      Destination Port :

Source MAC :      Local Routing Mark :

Ingress Interface	DSCP	Source IP	Destination IP	Source Port	Protocol	Local Mark	Delete
Dest Interface	CoS	Mask	Mask	Destination Port	Source MAC		

Apply    Cancel

**Figure 38: Policy Routing Configuration**

Field	Description
<b>Ingress Interface</b>	The incoming traffic interface for a Policy Routing rule. Selections include LAN interfaces, WAN interfaces, Locally generated (traffic) and not applicable. Examples of Locally generated traffic are: voice packets, packets generated by applications such as DNS, DHCP, etc.
<b>Destination Interface</b>	The outgoing traffic interfaces for a Policy Routing rule. Selections include LAN Interfaces and WAN interfaces.
<b>DiffServ Code Point</b>	The DiffServ Code Point (DSCP) field value ranges from 1 to 255. This field cannot be configured alone, additional fields like IP, Source MAC and/or Ingress Interface should be configured.
<b>Class of Service</b>	The selections are (in the order of priority): CoS1, CoS2, CoS3, CoS4, CoS5, CoS6 and N/A.
<b>Source IP</b>	The IP address of the traffic source.
<b>Mask</b>	The source IP Netmask. This field is required if the source IP has been entered.
<b>Destination IP</b>	The IP address of the traffic destination.
<b>Mask</b>	The Netmask of the destination. This field is required if the destination IP has been entered.
<b>Protocol</b>	The selections are TCP, UDP, ICMP, Specify and none. If you choose Specify, you need to enter the protocol number in the box next to the Protocol field. This field cannot be configured alone, additional fields like IP, Source MAC and/or Ingress Interface should be configured. This field is also required if the source port or destination port has been entered.
<b>Source Port</b>	The source protocol port. You cannot configure this field without entering the protocol first.
<b>Destination Port</b>	The destination protocol port or port range. You cannot configure this field without entering the protocol first.
<b>Source MAC</b>	The MAC address of the traffic source.
<b>Local Routing MAC</b>	<p>This field is enabled only when Locally Generated is selected in the Ingress Interface field. The mark for DNS traffic generated by different applications are described below:</p> <ul style="list-style-type: none"> <li>Dynamic DNS: 0xE1</li> <li>Dynamic Proxy: 0xE2</li> <li>Web Server: 0xE3</li> <li>MSNTP: 0xE4</li> <li>DHCP Server: 0xE5</li> <li>IP tables Utility: 0xE6</li> <li>PPP Deamon: 0xE7</li> <li>IP Route: 0xE8</li> <li>ATM Library: 0xE9</li> <li>NET Tools: 0xEA</li> <li>RIP: 0xEB</li> <li>RIP v2: 0xEC</li> <li>UPNP: 0xEE</li> <li>Busybox Utility: 0xEF</li> <li>Configuration Manager: 0xF0</li> <li>DropBear Utility: 0xF1</li> <li>Voice: 0</li> </ul>

Currently routing algorithms make decision based on destination address, i.e. only Destination IP address and subnet mask is supported. The Policy Routing page enables you to route packets on the basis of various fields in the packet.

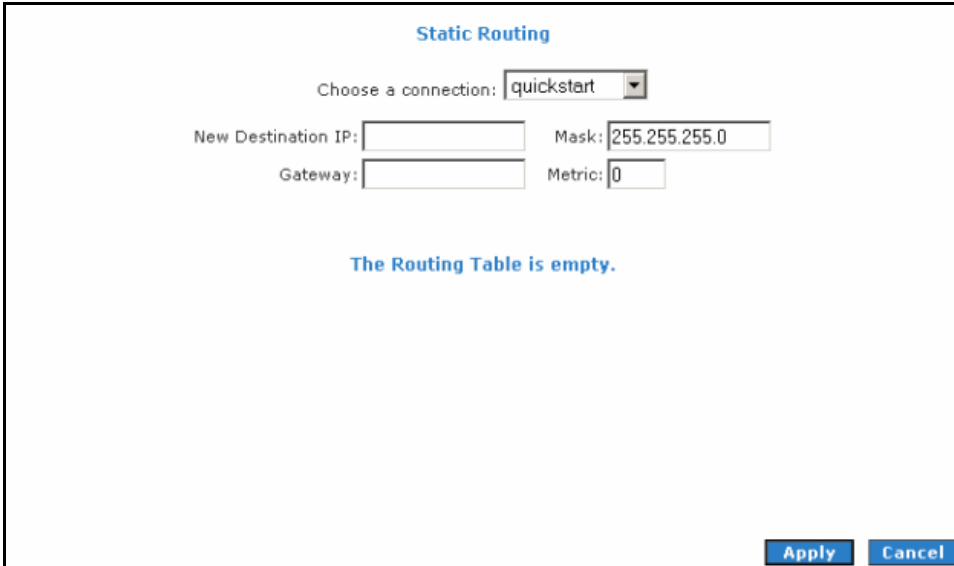
The following fields can be configured for Policy Routing:

- Destination IP address/mask
- Source IP address/mask
- Source MAC address
- Protocol (TCP, UDP, ICMP, etc)
- Source port
- Destination port
- Incoming interface
- DSCP

## Routing

### Static Routing

If the router is connected to more than one network, you may need to set up a static route between them. A static route is a pre-defined pathway that network information must travel to reach a specific host or network. You can use static routing to allow different IP domain users to access the Internet through the router.

A screenshot of a web-based configuration window titled "Static Routing". At the top, there is a dropdown menu labeled "Choose a connection:" with "quickstart" selected. Below this are four input fields: "New Destination IP:" (empty), "Mask:" (containing "255.255.255.0"), "Gateway:" (empty), and "Metric:" (containing "0"). In the center of the window, the text "The Routing Table is empty." is displayed in blue. At the bottom right, there are two buttons: "Apply" and "Cancel".

**Figure 39: Static Routing**

The New Destination IP is the address of the remote LAN or host to which you want to assign a static route. Enter the IP address of the host for which you wish to create a static route here. For a standard Class C IP domain, the network address is the first three fields of the New Destination IP, while the last field should be 0. The Subnet Mask identifies which portion of a IP address is the network portion and which portion is the host portion. For a full Class C Subnet, the Subnet Mask is 255.255.255.0. The Gateway IP address should be the IP address of the gateway device that allows for contact between the Gateway and the remote network or host.

## Routing Table

Routing Table displays the information used by routers when making packet-forwarding decisions. Packets are routed according to the packet's destination IP address.

Routing Table							
Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
220.255.161.1	0.0.0.0	255.255.255.255	UH	0	0	0	ppp0
192.168.1.0	0.0.0.0	255.255.255.0	U	0	0	0	br0
239.0.0.0	0.0.0.0	255.0.0.0	U	1	0	0	br0
0.0.0.0	220.255.161.1	0.0.0.0	UG	0	0	0	ppp0

Figure 40: Routing Table

## System Password

Anyone who can access the Web User Interface can be considered an Administrator. To restrict access to the Web User Interface, you need to set the System Password in the LAN Configuration page.

### Changing the System Password

To change the System Password:

1. Click the **Advanced** menu
2. Click **System Password**. This opens the **System Password** page.
3. Select **Enable Authentication**.
4. Enter your password.
5. Re-enter your password in the **Confirm Password** text box.
6. To temporarily implement the settings, click **Apply**.
7. To make changes permanent, click **Save Settings**.



Remember your account information. If you forget the Username and System Password, you will need to reset the router to its default settings. To reset, press and hold **RESET** at the router's back panel for 10 seconds..



## Changing the Timeout Settings

To change the timeout settings:

1. Click the **Advanced** menu
2. Click **System Password**.
3. Select **Enable Authentication**.
4. Enter the number of minutes in the **Idle Timeout** text field.
5. To temporarily implement the settings, click **Apply**.
6. To make changes permanent, click **Save Settings**.

## Firmware Upgrade

When updating the firmware, make sure you are using the correct file. Once the upgrade is complete, the router will reboot. You will need to log back into the router after the firmware upgrade is completed.

To update the firmware:

1. Click the **Advanced** menu then click **Firmware Upgrade**. This opens the **Firmware Upgrade** page.
2. Click **Browse** then locate the firmware file.
3. Click **Update Gateway**. The update may take a few minutes. Make sure that the power is not turned off during the update process.

## Restoring the Default Settings

To reset to the default factory settings, press and hold **RESET** for 10 seconds. This can be found at the router's back panel. When you reset, all the software updates will be lost.

To access the Web User Interface again, you need to install the router anew.

## Chapter 5: Security Menu

Security features include IP Filters and LAN isolation.



Figure 41: Security menu

### IP Filters

IP filtering allows you to block specific applications/services based on the IP address of the LAN device. In this page, you can block specific traffic (for example, block web access) or any traffic from a host on your local network.

A database of predefined IP filters allows you to apply one or more filtering rules to one or more members of a defined LAN group. You can view the rules associated with a predefined filter and add the available rules for a given category. You can also create, edit or delete your own IP filter rules.

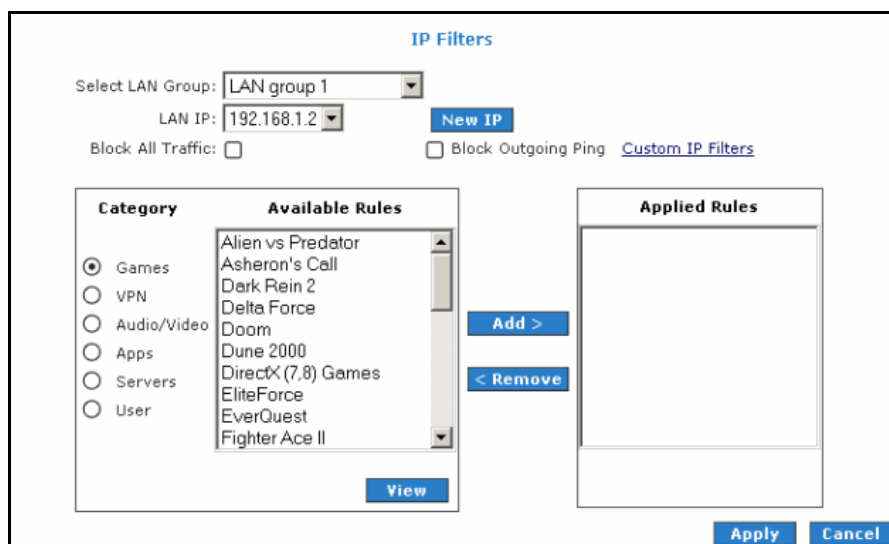


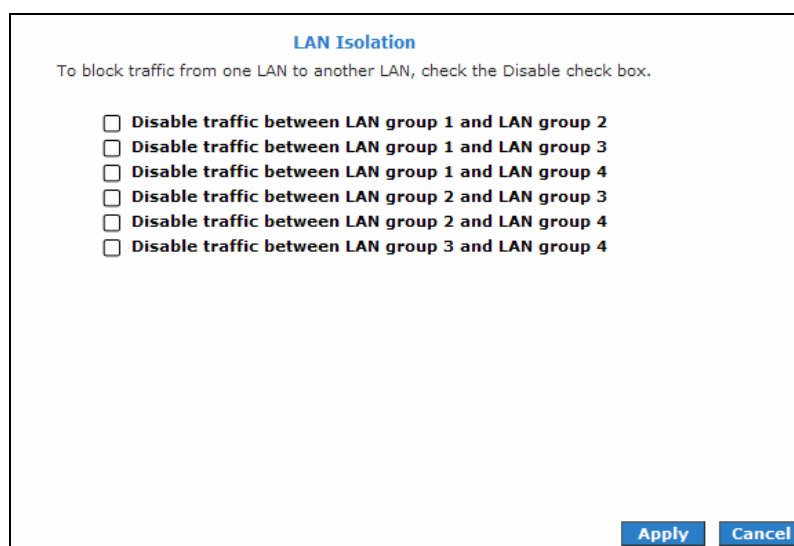
Figure 42: IP Filters

**To configure IP Filters:**

1. Click the **Security** menu then click **IP Filters**.
2. On the **IP Filters** page, select **LAN Group** and **LAN IP**. If the desired LAN IP is not available in the LAN IP drop-down menu, you can add it using the **LAN Client** page, which is accessed by clicking **New IP**.
3. Select the available rules for a given category. Click **View** to view the rule associated with a predefined filter. Click **Add** to apply the rule for this category.
4. If a rule is not in the list, you can create your own rule in the **User category**. Select **User** then click **New**.
5. The Rule Management page opens for you to create new rules. Enter **Rule Name**, **Protocol**, **Port Start**, **Port End** and **Port Map** then click **Apply**.  
The rules you create will appear in the **Available Rules** pane in the User category. You can view or delete the rules you create.
6. Continue to add rules as they apply from each category using the **Add** button.
7. To temporarily implement the changes, click **Apply**.
8. To make the change permanent, click **Save Settings**.

## LAN Isolation

LAN Isolation allows you to disable specific traffic connections between specific group. In this page, you can block specific traffic (for example, block LAN group I & group IV traffics) or any traffic from one group to another on your local network.



**LAN Isolation**

To block traffic from one LAN to another LAN, check the Disable check box.

- ☐ Disable traffic between LAN group 1 and LAN group 2
- ☐ Disable traffic between LAN group 1 and LAN group 3
- ☐ Disable traffic between LAN group 1 and LAN group 4
- ☐ Disable traffic between LAN group 2 and LAN group 3
- ☐ Disable traffic between LAN group 2 and LAN group 4
- ☐ Disable traffic between LAN group 3 and LAN group 4

**Apply** **Cancel**

**Figure 43: LAN Isolation**

## Chapter 6: Status Menu

This chapter provides information about monitoring the router status and viewing product information. Your router allows you to view the following status and product information:

- Connection Status
- System Log
- Remote Log
- Network Statistics
- DHCP Clients
- QoS Status
- Modem Status
- Product Information

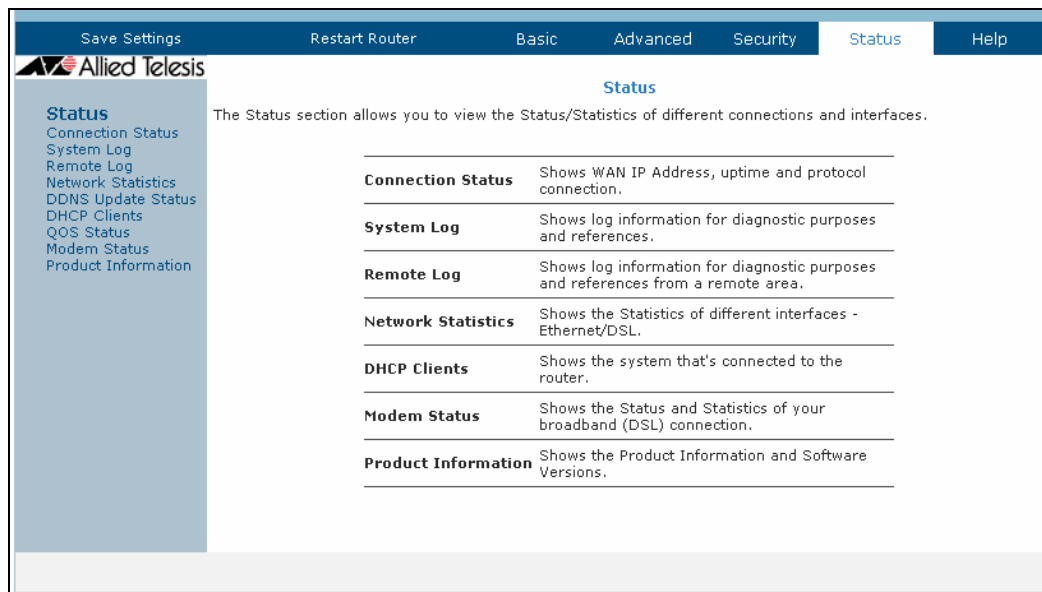


Figure 44: Status menu

## Connection Status

Connection Status displays the type of protocol, the WAN IP address, the connection state and the duration of your Internet connection. To view the Connection Status, go to the **Status** menu then click **Connection Status**.



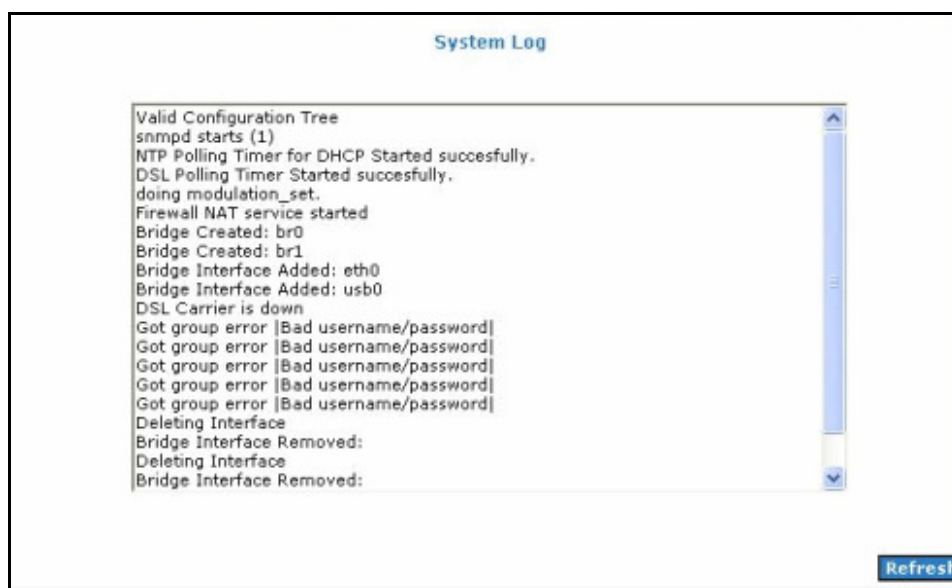
Description	Type	IP	State	Online	Disconnect Reason
quickstart	pppoe	N/A	Not Connected	0	DSL Line is Disconnected

Refresh

Figure 45: Connection Status

## System Log

System Log displays the router log. Depending on the severity level, the information log will generate log reports to a remote host if remote logging is enabled. To view the System Log, go to the **Status** menu then click **System Log**.



Valid Configuration Tree
snmpd starts (1)
NTP Polling Timer for DHCP Started succesfully.
DSL Polling Timer Started succesfully.
doing modulation_set.
Firewall NAT service started
Bridge Created: br0
Bridge Created: br1
Bridge Interface Added: eth0
Bridge Interface Added: usb0
DSL Carrier is down
Got group error [Bad username/password]
Got group error [Bad username/password]
Got group error [Bad username/password]
Got group error [Bad username/password]
Got group error [Bad username/password]
Deleting Interface
Bridge Interface Removed:
Deleting Interface
Bridge Interface Removed:

Refresh

Figure 46: System Log

## Remote Log

Remote Log allows you to forward all logged information to one (or more) remote computer. The type of information forwarded to the remote computer depends on the Log level. Each log message belongs to a certain log level, which indicates the severity of the event.

When you configure remote logging, you must specify a severity level. Log messages that are rated at that level or higher are sent to the log server and can be viewed using the server log application, which can be downloaded from the web.

**Figure 47: Remote Log Settings**

### To enable remote logging:

1. Go to the **Status** menu then click **Remote Log**.
2. Select a **Log Level**. There are 8 log levels listed below in order of severity.
  - **Panic** System panic or other condition that causes the router to stop functioning.
  - **Alert** Conditions that require immediate correction, such as a corrupted system database.
  - **Critical** Critical conditions such as hard drive errors.
  - **Error** Error conditions that generally have less serious consequences than errors in the emergency, alert and critical levels.
  - **Warning** Conditions that warrant monitoring.
  - **Notice** (Default) Conditions that are not errors but might warrant special handling.
  - **Info** Events or non-error conditions of interest.
  - **Debug** Software debugging message. Specify this level only when directed by a technical support representative.
3. Enter the **IP Address** where the log will be sent to then click **Add**.
4. Click **Apply**. The IP address will appear in the **Select a logging destination** drop- down menu.
5. To make changes permanent, click **Save Settings**.



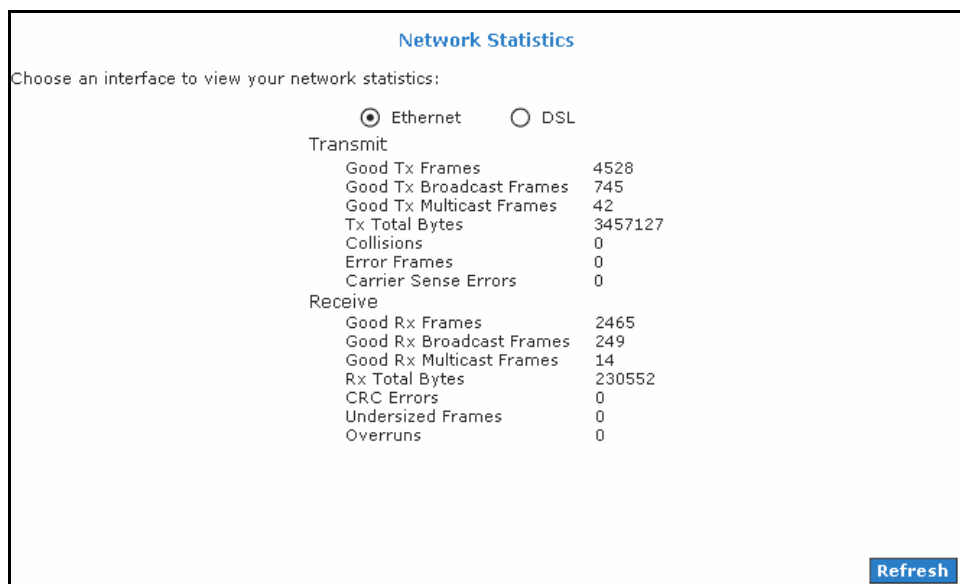
*When you select a log level, all log information within this severity level and levels above (meaning, more severe levels) will be sent to the remote host.*

**To disable a remote log:**

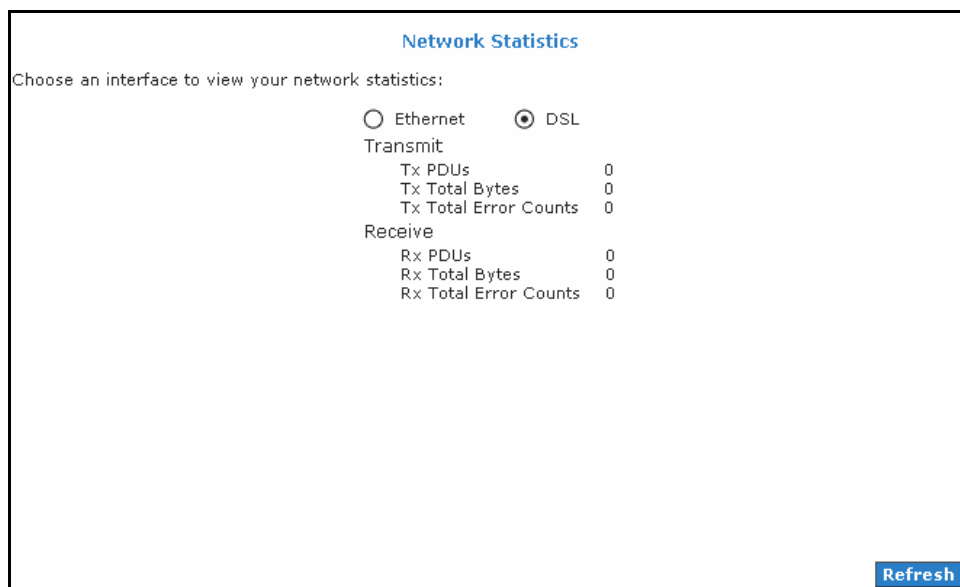
1. Select the IP address to be deleted from the **Select a logging destination** drop-down menu.
2. To temporarily implement the changes, click **Apply**.
3. To make changes permanent, click **Save Settings**.

## Network Statistics

The Ethernet and DSL statuses are displayed in this page. To view the Network Statistics, go to the **Status** menu then click **Network Statistics**.



**Figure 48: Network Statistics – Ethernet**



**Figure 49: Network Statistics – DSL**

## DHCP Clients

DHCP Clients displays the MAC Address, IP Address, Host Name and Lease Time. To view the DHCP Clients, go to the **Status** menu then click **DHCP Clients**.

DHCP Clients (1)			
Select LAN: LAN group 1			
MAC Address	IP Address	Host Name	Lease Time
00:10:b5:6d:e5:13	192.168.1.2	PhuahHongWen	0 days 0:39:8
Refresh			

Figure 50: DHCP Clients

## QoS Status

This page displays the Quality of Service and the packet statistics. To view the QoS Status, go to the **Status** menu then click **QoS Status**.

QOS STATUS	
QOS Framework : Enabled	
Scheduling Algorithm : Strict Round-Robin	
<b>NQM Received Statistics</b>	<b>NQM Dropped Statistics</b>
Cos1 Pkts received : 0	Cos1 Pkts received : 0
Cos2 Pkts received : 0	Cos2 Pkts received : 0
Cos3 Pkts received : 0	Cos3 Pkts received : 0
Cos4 Pkts received : 0	Cos4 Pkts received : 0
Cos5 Pkts received : 0	Cos5 Pkts received : 0
Cos6 Pkts received : 8015	Cos6 Pkts received : 0
<b>NQM Congestion Control</b>	<b>Translation Statistics</b>
Cos1 Queue : Empty	Packets Remarkd : 0
Cos2 Queue : Empty	Packets Unchanged : 0
Cos3 Queue : Empty	Non-Ip Packets Marked : 0
Cos4 Queue : Empty	Unclassified Ip Packets Marked : 0
Cos5 Queue : Empty	Unclassified Non-Ip Packets Marked : 0
Cos6 Queue : Empty	Unclassified Layer2 Packets : 0
Congestion State : Not Congested	
<b>Classification Statistics</b>	
Classification Errors : 0	
UnClassified Packets : 0 Fragmented Packets = 0	

Figure 51: QoS Status



## Modem Status

This page displays the model status. To view the Modem Status, go to the **Status** menu then click **Modem Status**.

Modem Status	
Modem Status	
Connection Status	Connected
Us Rate (Kbps)	512
Ds Rate (Kbps)	3488
US Margin	25
DS Margin	22
Trained Modulation	ADSL_G.dmt
LOS Errors	0
DS Line Attenuation	34
US Line Attenuation	21
Peak Cell Rate	1207 cells per sec
CRC Rx Fast	0
CRC Tx Fast	1
CRC Rx Interleaved	0
CRC Tx Interleaved	0
Path Mode	Fast Path
DSL Statistics	
Near End F4 Loop Back Count	0
Near End F5 Loop Back Count	0
<a href="#">Refresh</a>	

Figure 52: Modem Status

## Product Information

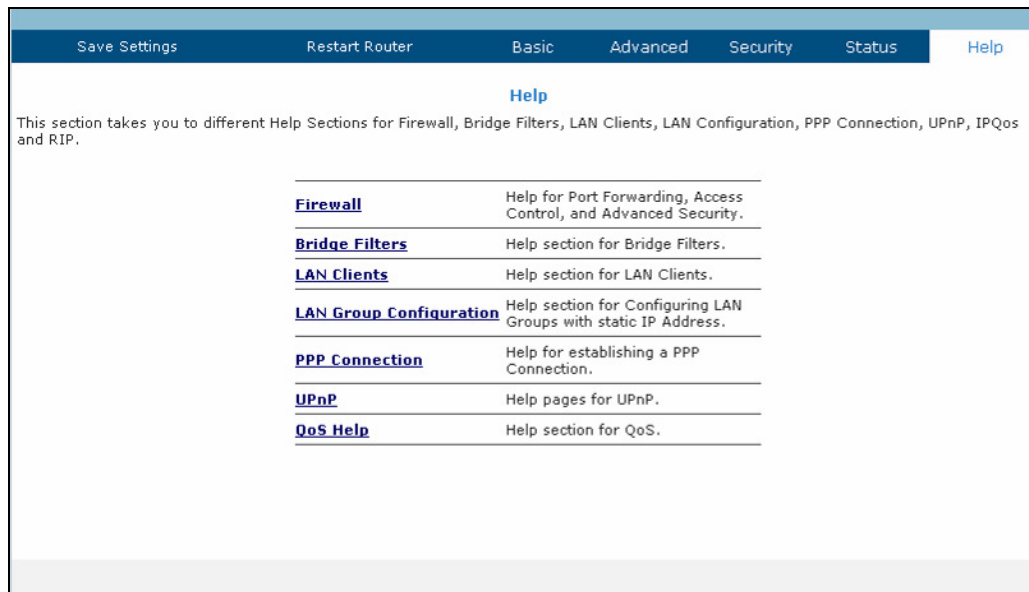
This page displays the product information and software versions. To view the Product Information, go to the **Status** menu then click **Product Information**.

Product Information	
Product Information	
Model Number	AT-AR256E v3
Ethernet MAC	00:30:0A:96:D4:52
DSL MAC	00:30:0A:96:D4:53
Software Versions	
Gateway	3.7.0
Firmware	119.12a.1-006
ATM Driver	6.00.01.00
DSL HAL	6.00.01.00
DSL Datapump	6.00.04.00 Annex A
SAR HAL	01.07.2b
PDSP Firmware	0.54
Boot Loader	1.4.0.4

Figure 53: Product Information

## Chapter 7: Help Menu

The Help page provides documentation for various topics like Firewall, Bridge Filters, LAN Clients, LAN Group Configuration, PPP Configuration, IP QoS and Routing Information Protocol. To access Help, click the **Help** menu.



**Figure 54: Help menu**

In order to obtain help on a topic, click on the relevant command.